北京大学数学丛书

代　数　学

上　册

莫宗坚　蓝以中　赵春来　著

北京大学出版社

内 容 提 要

本书分上、下两册出版。

上册主要讲述近世代数的初步知识，内容包括集合论与数论、群论、多项式论、线性代数以及域论。

本书内容丰富，直观性强，推理自然，解释详尽。此书的独到之处是特别注重对于代数学的背景、基本思想以及与其它学科的联系等方面的介绍。书中精选了大量的例题和习题。本书的起点低，由浅入深。具有高等代数基础知识的读者就可以阅读本书，进而学到现代代数学的较大部分基础知识。

本书可作为高等学校数学系高年级学生以及研究生的教材，也可供数学工作者参考。

北京大学数学丛书

代 数 学

上 册

莫宗坚 等著

•

北京大学出版社出版

（北京大学校内）

北下关印刷厂印刷

新华书店北京发行所发行 各地新华书店经售

850×1168毫米 32开本 12印张 302千字

1986年10月第一版 1987年10月第二次印刷

印数：12001—17500册

统一书号：13209 · 140 定价：2.95元

上册目录

第一章　集合论与数论

§1　集　合　论

我们假定读者已熟悉集合论的基本概念，如**交集**、**并集**、**子集**、**包含**及**映射**等．请参考前面的“符号说明”．

定义1.1　设S及T为集合，$\rho: S \to T$是由S到T的映射．任取S中的二元素s_1及s_2，如果$\rho(s_1)=\rho(s_2)$时，必有$s_1=s_2$，则称ρ为**一一映射**，或**单射**．如果对于T中任意元素t，必有$s\in S$，使$\rho(s)=t$，则称ρ为S到T**上**的映射，或**满射**．如果ρ同时为单射及满射，则称ρ为**单满映射**．

集合论中最有意义的概念之一是“基数”．我们有如下的定义：

定义1.2　设S及T为集合．如有一单满映射$\rho: S\to T$，则称S与T**同基数**．

讨论　1）如集合S与整数集合$\{1,2,\cdots,n\}$同基数，则称S为**有限集**，而称其基数为n．反之则称之为**无限集**．设S及T为同基数的有限集，$\rho: S\to T$为一映射，则易证：如ρ为单射，则ρ必为满射．反之，如ρ为满射，则ρ必为单射．此一命题可谓之**鸽笼定理**，即设想S为一群鸽子，T为等数的鸽笼，则上命题即：如果每一鸽子已一一进笼，则鸽笼必无空者；反之，如鸽笼皆无空者，则必然每一笼中仅有一只鸽子．

2）如集合S与正整数集合$\{1,2,3,\cdots,n,\cdots\}$同基数，则称$S$为**可数无限集**．有限集与可数无限集统称**可数集**．除此之外，皆称为**不可数集**．

3）对所有的无限集而言，鸽笼定理皆不成立，然而证法比较

复杂，远离本书的趣旨，请读者参考集合论的专书。现在我们仅举一例以说明此种现象，即所谓的“希尔伯特的旅馆”：设一旅馆有可数无限个房间$\{1,2,\cdots,n,\cdots\}$，已住满房客。如同时又来了可数无限个新房客$\{g_1,g_2,\cdots,g_n,\cdots\}$，则一个简易的安排方法是令原住$n$号房间的老房客移入$2n$号房间，于是空出$\{1,3,5,\cdots,2n+1,\cdots\}$所有奇数号房间。令新房客依序住入即可，也即令新房客g_n住入$2n-1$号房间。从此例中，可以看出单射不一定必是满射。反之，如令头两个人挤一间房，其余的人依序住入空出的房间，则满射又不一定是单射了。

定理1.1 有理数集Q是可数无限集。

证明 我们采用所谓“三角数法”。考虑正有理数的集合Q_+。把Q_+中的元素按分母大小排成如下的无限矩阵：

$$Q_+=\begin{pmatrix} \frac{1}{1} & \frac{2}{1} & \frac{3}{1} & \cdots\cdots \\ \frac{1}{2} & \frac{2}{2} & \frac{3}{2} & \cdots\cdots \\ \frac{1}{3} & \frac{2}{3} & \frac{3}{3} & \cdots\cdots \\ \cdots & \cdots & \cdots & \cdots \\ \frac{1}{n} & \frac{2}{n} & \frac{3}{n} & \cdots\cdots \\ \cdots & \cdots & \cdots & \cdots \end{pmatrix},$$

然后我们把整个矩阵的元素，按箭头所指的顺序，依次对应到所有正的偶数，自然，已经出现过的有理数则略去。例如，

$$\frac{1}{1}\to 2,\ \frac{1}{2}\to 4,\ \frac{2}{1}\to 6,\ \frac{1}{3}\to 8,\ \frac{3}{1}\to 10,$$

等等。这样就把Q_+对应到了正偶数集。同法，我们可以把负有理数集Q_-对应到大于1的正奇数集。再把0对应到1。不难看出，这个对应是由Q到正整数集$N=\{1,2,\cdots,n,\cdots\}$的单满映射。

于是Q是可数无限集。∎

系 设有可数集$S_i=\{s_{i1},s_{i2},\cdots,s_{in},\cdots\}$，$i\in$可数集$I$。则这些可数个$S_i$的并集$\bigcup_{i\in I}S_i$也是可数集。

证明 利用三角数法。∎

定理1.2 实数集$\boldsymbol{R}$为不可数集。

证明 假设$\boldsymbol{R}$为可数集，则所有实数可以排成一行：$\{r_1,r_2,\cdots,r_n,\cdots\}$。我们用"对角线法"来证明这是不可能的。

把$r_1,r_2,\cdots,r_n,\cdots$用十进小数写出如下：

$$r_1=a_1.b_{11}\,b_{12}\cdots b_{1n}\cdots,$$
$$r_2=a_2.b_{21}\,b_{22}\cdots b_{2n}\cdots,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$r_n=a_n.b_{n1}\,b_{n2}\cdots b_{nn}\cdots,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

其中诸a_i为整数，b_{ij}为$0,1,2,\cdots,9$之一。现取一实数

$$r=0.c_1\,c_2\cdots c_n\cdots$$

如下：如果$b_{nn}\neq 5$，则取$c_n=5$，否则取$c_n=4$（$n=1,2,\cdots$）。显然$r\neq r_n$（$\forall n=1,2,\cdots$）。故r不在集合$\{r_1,r_2,\cdots,r_n,\cdots\}$之中。由此知$\boldsymbol{R}$为不可数集。∎

在代数学中，经常应用构造"直积"、"商集"的方法。我们有如下定义。

定义1.3 设I为一个集合。如果对每一个$i\in I$，都有一个集合S_i，则S_i的直积$\prod_{i\in I}S_i$定义为

$$\{(s_i)_{i\in I}:\ s_i\in S_i\},$$

即I到$\bigcup_{i\in I}S_i$的所有映射s，而且能适合$s(i)=s_i\in S_i$者。如I为可数集时，$\prod_{i\in I}S_i$中的元素常写成一行$(s_1,s_2,\cdots,s_n,\cdots)$。

定义1.4 设T为一集合。如果T为一些分离的子集的并集，

即$T=\bigcup_{j\in I}T_j$，并且不同的子集T_j的交集为空集，则这些子集T_j的集合$\{T_j: j\in J\}$称为T的一个**商集**。

讨论 1）设T为所有中国人民的集合，按照某种法定年龄的标准，T可以划分为T_1=未成年人的集合和T_2=成年人的集合。则$\{T_1,T_2\}$构成T的一个商集。此商集中仅有两个元素。

2）设$\{T_j: j\in I\}$为T的一个商集，则可在T中定义一个相应的"等价关系"～如下：

$$a\sim b \iff a,b\text{属于同一个}T_j.$$

一般言之，任意关系"～"如具有下列三条性质，则称为一个**等价关系**：

(a) 反身性：$a\sim a$；

(b) 对称性：如果$a\sim b$，则$b\sim a$；

(c) 传递性：如果$a\sim b$，$b\sim c$，则$a\sim c$。▎

我们也可以用等价关系来定义商集如下。

定义1.4* 设～为集合T上的等价关系。令

$$T_a=\{b: b\in T,\ b\sim a\},$$

则$\{T_a: a\in T\}$是T的一个商集，称之为**关于等价关系～的商集**，T_a称为一个**等价子集**。

讨论 为说明定义1.4*中的$\{T_a\}$确实是商集，我们仅须验证两点：1）$T=\bigcup_{a\in T}T_a$；2）如果$T_a\cap T_c\neq\varnothing$，则$T_a=T_c$。1）是显然的，这因为$a\sim a$，所以$a\in T_a$；关于2），设$b\in T_a\cap T_c$，令$d$为$T_c$中任意元素，则有

$$a\sim b\sim c\sim d,\quad a\sim c\sim d,\quad a\sim d.$$

即$d\in T_a$。所以$T_c\subset T_a$。同法可得出$T_a\subset T_c$，于是$T_a=T_c$。▎

下面的"数学归纳法"是正整数集N的公理之一，其详情请见附录中正整数的"皮诺公理"。

数学归纳法 设对每个正整数m，有命题$P(m)$。如能证明：

1） $P(1)$是正确的；

2） 设n是任意大于1的正整数．如对所有小于n的正整数l，$P(l)$都是正确的，则$P(n)$是正确的，

那么所有的命题$P(m)$皆是正确的．

讨论 这个数学归纳法不能从更简明的公理系统导出，然而可以从下面的讨论中理解其合理性：根据1)，已知$P(1)$是正确的．运用2)，令$n=2$，则知$P(2)$是正确的．再运用2)，令$n=3$，则知$P(3)$是正确的．如此反复运用2)，则知所有的命题$P(m)$皆是正确的．❙

在代数学里，经常应用"Zorn引理"．此引理等同于"选择公理"及"良序原理"，是集合论的公理之一．为了讨论Zorn引理，我们先引入"序"与"半序"的概念．

定义1.5 设S为一集合．S的一个关系"$\geqslant$"如适合下列条件，则称之为一个**半序**：

1） $s_1\geqslant s_1$， $\forall s_1\in S$；

2） $s_1\geqslant s_2$， $s_2\geqslant s_3 \Longrightarrow s_1\geqslant s_3$， $\forall s_1,s_2,s_3\in S$；

3） $s_1\geqslant s_2$， $s_2\geqslant s_1 \Longrightarrow s_1=s_2$， $\forall s_1,s_2\in S$.

定义1.6 设S为一集合，$\geqslant$为S的半序．如果适合下列条件，则称$\geqslant$为S的**序**：

4） 对任意的$s_1,s_2\in S$，总有$s_1\geqslant s_2$或$s_2\geqslant s_1$.

定义1.7 设$\geqslant$为S的半序，T为S的子集．如果S的一个元素s，适合$s\geqslant t$（$\forall t\in T$），则称s为T的一个**上限**．如果s具有如下性质：$\forall s_1\in S$，只要$s_1\geqslant s$，必有$s_1=s$，则称s为S的一个**极大元素**．

定义1.8 设S为一集合，$\geqslant$为S的半序，T为S的子集．如果局限于T中$\geqslant$是一个序，则称T为一**链**．

Zorn引理 设S为一非空集合，$\geqslant$为S的半序．如果任意链皆有上限，则S有一极大元素．

讨论 1） 在集合论中，已经证明了Zorn引理实际上是一个

公理，所以不可能从其它较简单的公理系统中导出。

2）利用Zorn 引理可以简化许多证明，也可以证明一些除此之外的其它方法不能证明的结果。例如，我们可以证明平面上的任何有界区域D内皆有极大的开圆盘，证法如下：(a) 令S为D内所有开圆盘构成的集合，用包含$\subset$定义半序$\leqslant$；(b) 由于D内至少有一个开圆盘，所以S是非空的；(c) 如果一些开圆盘构成的集合$\{D_i: i\in I\}$成为一链，则$\bigcup_{i\in I} D_i$也显然是D的一个开圆盘，它是此链的上限；(d) 于是根据Zorn 引理，有界区域D内必有极大的开圆盘。

习　题

1. 设ρ为集合S到集合T的映射。证明ρ是一个单射的充要条件是下列两条件中任一条成立：

(1) 存在T到S的映射τ，使$\tau\rho = 1_S$；

(2) 不存在某集合U到S的两个不同映射τ_1,τ_2，使

$$\rho\tau_1 = \rho\tau_2.$$

2. 设ρ为集合S到集合T的映射。证明ρ是一个满射的充要条件是下列两条件中任一条成立：

(1) 存在T到S的映射τ，使$\rho\tau = 1_T$；

(2) 不存在T到某集合U的两个不同映射τ_1,τ_2，使

$$\tau_1\rho = \tau_2\rho.$$

3. 设S是一基数为$n(n\geqslant 1)$的有序集。证明在S中存在一个元素a，使$\forall b\in S$，有$a\leqslant b$。举例说明无限的有序集不一定具有此性质。

4. 设ρ是集合S到集合T的映射，A,B是S的子集。证明

$$\rho(A\cup B) = \rho(A)\cup\rho(B),\qquad \rho(A\cap B)\subset\rho(A)\cap\rho(B).$$

举例说明$\rho(A\cap B)$不一定等于$\rho(A)\cap\rho(B)$。

5. 设ρ是集合S到集合T的映射，A是S的子集。证明在

一般情况下 $\rho(S\backslash A)\subsetneq T\backslash\rho(A)$。

6. 设$\omega_1,\omega_2\in \boldsymbol{C}$，且$\omega_1/\omega_2\overline{\in}\boldsymbol{R}$。在$\boldsymbol{C}$内定义等价关系：

$$\alpha\sim\beta \iff \beta=\alpha+a\omega_1+b\omega_2 \quad (a,b\in \boldsymbol{Z})。$$

试求$\boldsymbol{C}$对上述等价关系的商集。

7. 令$\boldsymbol{Q}[x]$表示所有有理系数的多项式集。证明$\boldsymbol{Q}[x]$是一个可数集。

8. 令C表 Cantor 点集。C的构造法如次：在区间$[0,1]$中挖去中间的1/3长的开线段$(1/3,2/3)$。其次，在所余的两个闭线段$[0,1/3]$，$[2/3,1]$中各挖去中间的 1/3 长的开线段。如此反复作下去，所得的余集即是C。证明C是一个不可数集。

9. 证明“兄弟”是一个等价关系，“子女”不是一个等价关系。

10. 证明在整数集$\boldsymbol{Z}$中，通常用的“$\geqslant$”是一个序。

11. 证明在任何一个集合S中，包含“$\supset$”是子集族的一个半序。

12. 证明题10中的半序不适合Zorn 引理的条件，而题 11 中的半序适合之。

§2 唯一分解定理

数学的起源之一是对整数的研究。近世代数从整数的“皮诺公理系”开始讨论，由此公理系引出整数集的四则运算的法则，如交换律、结合律、分配律等，并进一步建构有理数集$\boldsymbol{Q}$、实数集$\boldsymbol{R}$、复数集$\boldsymbol{C}$。这种讨论法自有其逻辑的严谨性，然而对于代数学的读者而言，似嫌迂远，旁离本旨。本书将这部分的推理列入附录中。以下我们将假设读者已熟悉整数集$\boldsymbol{Z}$、有理数集$\boldsymbol{Q}$、实数集$\boldsymbol{R}$及复数集$\boldsymbol{C}$的四则运算的法则。

整数论中，最重要的定理之一是“辗转相除法”。汉代的数学书《九章算术》中，有求两正整数的公因数的“更相减损求

等”之法，即“辗转相除法”也。秦九韶于《数书九章》（1247年）又曾论及。在现代，此法通常被称为“欧几里得算法”。我们先引入如下的概念。

定义1.9 设a为一实数，以$[a]$表示小于或等于a的最大整数，即a的**整数部分**。

讨论 例如，$[3.1]=3$，$[-3.1]=-4$，$[5]=5$。

定理1.3（欧几里得算法） 令d为一正实数，n为任意实数。则必有一整数q及一实数r，使得

$$n=qd+r, \quad 0\leqslant r<d.$$

证明 应用定义1.9，读者自证。▎

系1 在以上定理中，q及r皆为唯一确定的。

证明 读者自证。▎

系2 如在上定理中n及d皆为整数，则r也为整数。

欧几里得算法的应用之一是研究几个整数的因数及公因数。为此，我们定义如下：

定义1.10 设a,b,c为整数。如果$a=bc$，则称a是b的**倍数**，b是a的**因数**，用符号$b|a$表示之。如果$b|a_1,b|a_2,\cdots,b|a_n$，则称b是$a_1,a_2,\cdots,a_n$的**公因数**。$a_1,a_2,\cdots,a_n$的公因数中的最大者，称为$a_1,a_2,\cdots,a_n$的**最大公因数**。如果$b_1|a,b_2|a,\cdots,b_m|a$，则称a是$b_1,b_2,\cdots,b_m$的**公倍数**。$b_1,b_2,\cdots,b_m$的公倍数中最小非负整数，称为$b_1,b_2,\cdots,b_m$的**最小公倍数**。如果a与b的最大公因数是1，则称a与b**互素**。

定理1.4 设$a_1,a_2\in \mathbf{Z}$，且a_1,a_2不全为零，则a_1,a_2的最大公因数是集合

$$(a_1,a_2)=\{b_1a_1+b_2a_2:\ b_1,b_2\in \mathbf{Z}\}$$

中的最小正整数。

证明 令集合(a_1,a_2)中的最小正整数为

$$d=c_1a_1+c_2a_2, \quad c_1,c_2\in \mathbf{Z}.$$

按照欧几里得算法，存在整数 q_1 及 r_1，使得

$$a_1 = q_1 d + r_1, \qquad 0 \leqslant r_1 < d.$$

如果 $r_1 \neq 0$，则有

$$r_1 = a_1 - q_1 d = (1 - c_1 q_1) a_1 + (-q_1 c_2) a_2 \in (a_1, a_2),$$

即 r_1 是 (a_1, a_2) 中比 d 更小的正整数。这显然是不可能的。故知 $r_1 = 0$，即

$$a_1 = q_1 d,$$

亦即

$$d \mid a_1.$$

同法可证 $d \mid a_2$。即 d 是 a_1, a_2 的公因数。

现设 d' 为 a_1, a_2 的另一公因数，则有

$$d' \mid a_1,\ d' \mid a_2 \implies d' \mid c_1 a_1 + c_2 a_2,$$

即 $d' \mid d$。而 d 为正整数，故 $d \geqslant d'$。 ▎

以下，我们将证明"算术基本定理"。即整数分解成"素数"的连乘积的"唯一分解定理"。为此，我们要引入"不可约数"及"素数"的概念。值得注意的是，在整数集中有乘法逆元素的数仅是 1 与 -1，即如果 n 与 n^{-1} 皆为整数，则 n 必为 1 或 -1。

定义 1.11 设有一整数 a，非 $0, 1, -1$。如在 a 的任意分解式 $bc = a$ 中，必有 b 或 c 为 1 或 -1(即 b 和 c 之一必为可逆的)，则称 a 是一个**不可分解数**(或称**不可约数**)。如果 $a \mid fg$ 时，必有 $a \mid f$ 或 $a \mid g$，则称 a 是一个**素数**。素数又称为**质数**。

引理 $\boldsymbol{Z}$ 的不可约数皆是素数，素数也皆是不可约数，

证明 设 a 是不可约数，不妨设 $a > 0$(否则讨论 $-a$)。设 $a \mid bc$。如果 a 不是 b 的因数，由于 a 的正因数只有 1 与 a，所以 a, b 的最大公因数必为 1。按照定理1.4，有 $c_1, c_2 \in \boldsymbol{Z}$，使得

$$1 = c_1 a + c_2 b.$$

以 c 乘上式两边，得到

$$c=c(c_1a+c_2b)=\left(cc_1+c_2\left(\frac{bc}{a}\right)\right)a.$$

由于$a|bc$，故$bc/a\in\boldsymbol{Z}$。由上式即知$a|c$。所以a为素数。反之，设a为素数，且$a=bc$。不妨设$a|b$，则a,b的最大公因数必为$|a|$及$|b|$，于是有$|a|=|b|$，故$c=\pm1$。▮

讨论 从上面的引理可以看出，在$\boldsymbol{Z}$中"不可约数"与"素数"是一物的二名。在以后的"环论"中可以看到，在广泛的情况下，这两个概念是各有所指的。这两个概念的同一性是下面的"唯一分解定理"的基石。

定理1.5(唯一分解定理) 任意大于1的整数a皆可分解成正素数的连乘积

$$a=\prod_i p_i.$$

在这个连乘积中，正素数p_i的次序自然可以调换。除此之外，这个连乘积是唯一的。

证明 我们首先证明这个分解是存在的，然后再证明其唯一性。

2是正素数，于是$2=2$是2的分解。按照数学归纳法，给定一个正整数$a>1$，可以假定所有大于1小于a的整数皆可分解。如果a是素数，则$a=a$是a的分解；如果a不是素数，应用引理，得到

$$a=bc,\quad a>b>1,\quad a>c>1,$$

其中b及c皆可分解成正素数连乘积，于是a可分解为正素数连乘积，即$a=\prod_i p_i$。

下面证分解的唯一性。设$a=\prod_j q_j$是a的另一正素数连乘积分解式，则有

$$p_1|a=q_1\left(\prod_{j>1}q_j\right),$$

于是有

$$p_1|q_1 \quad 或 \quad p_1\Big|\Big(\prod_{j>1}q_j\Big).$$

如果$p_1 \nmid q_1$，则必有$p_1\Big|q_2\Big(\prod_{j>2}q_j\Big)$，于是有

$$p_1|q_2 \quad 或 \quad p_1\Big|\Big(\prod_{j>2}q_j\Big).$$

如此推演下去，必有某个q_s，使得

$$p_1|q_s.$$

而q_s为素数，由引理，q_s为不可约数，于是有

$$q_s=p_1.$$

考虑

$$\prod_{i>1}p_i=\frac{a}{p_1}=\frac{a}{q_s}=\prod_{j\neq s}q_j,$$

应用数学归纳法，即有唯一性。∎

以后，除特别声明外，所谓"素数"皆指正素数而言。

例1 不难导出下述命题："设p_i $(i=1,2,\cdots,n)$均为素数，则$\Big(\prod_{i=1}^{n}p_i\Big)+1$的因数皆非$p_1,p_2,\cdots,p_n$。"这是因为，如果$p_j$为$\Big(\prod_{i=1}^{n}p_i\Big)+1$的因数，则有$a\in \boldsymbol{Z}$，使得

$$ap_j=\Big(\prod_{i=1}^{n}p_i\Big)+1,$$

即

$$\Big(a-\prod_{i\neq j}p_i\Big)p_j=1,$$

也即$p_j|1$。这显然是不可能的。由上面这个命题，又可推出"素数有无限多个"。事实上，如果仅有有限多个素数$p_1,p_2,\cdots,p_n$，

则$\left(\prod_{i=1}^{n} p_i\right)+1$的素因子只能是$p_1, p_2, \cdots, p_n$中的某些个，这与上面的命题矛盾。故知素数有无限多个。

例2 取一正分数m/n，可以用欧几里得算法求得其连分数。我们且举祖冲之(430—501年)的"密率"$\frac{355}{113}$为例。

$$\frac{355}{113}=\frac{3\times113+16}{113}=3+\frac{16}{113}=3+\cfrac{1}{\frac{113}{16}}$$

$$=3+\cfrac{1}{\frac{7\times16+1}{16}}=3+\cfrac{1}{7+\cfrac{1}{16}}.$$

更一般地，任意实数r，都可以用此法求出其连分数。我们以$\pi=3.14159265358979323846\cdots$为例，以说明之。

$$\pi=\frac{\pi}{1}=3+\frac{0.14159265358979323846\cdots}{1}$$

$$=3+\cfrac{1}{\cfrac{1}{0.14159265358979323846\cdots}}$$

$$=3+\cfrac{1}{7+\cfrac{0.00885142787144737077\cdots}{0.14159265358979323846\cdots}}$$

$$=3+\cfrac{1}{7+\cfrac{1}{\cfrac{0.14159265358979323846\cdots}{0.00885142787144737077\cdots}}}$$

$$=3+\cfrac{1}{7+\cfrac{1}{15+\cfrac{0.00882123551809317691\cdots}{0.00885142787144737007\cdots}}}$$

$$=3+\cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{1+\cfrac{0.0088514278714473 7007\cdots}{0.0000301923533541 9316\cdots}}}}$$

$$=3+\cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{1+\cfrac{1}{292+\cdots}}}}.$$

这种连分数与“最佳渐近分数”有关，详见华罗庚著《数论导引》第十章。在上面的π的连分数中，如果我们只保留前边几项，弃去其余的项，则得到

$$3,\quad 3+\frac{1}{7},\quad 3+\cfrac{1}{7+\cfrac{1}{15}},\quad 3+\cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{1}}},$$

$$3+\cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{1+\cfrac{1}{292}}}},$$

也即

$$3,\quad \frac{22}{7},\quad \frac{333}{106},\quad \frac{355}{113},\quad \frac{103993}{33102},$$

而祖冲之的“密率”适在其中。

习　题

1．设n为正整数，a为实数。证明：

（1）$\left[\frac{[na]}{n}\right]=[a]$；

(2) $[\alpha]+\left[\alpha+\frac{1}{n}\right]+\cdots+\left[\alpha+\frac{n-1}{n}\right]=[n\alpha]$.

2. 设$\alpha,\beta\in\boldsymbol{R}$。证明：

$$[2\alpha]+[2\beta]\geqslant[\alpha]+[\alpha+\beta]+[\beta].$$

3. 设a,b是两个正整数。证明它们的最大公因子d与最小公倍数m之积$dm=ab$。

4. 设n是一个正整数，p是一个素数。求$n!$的素因子标准分解式中p的方幂数。

5. 用欧几里得计算法证明：每一个正整数都可以用十进位法唯一地表示出。

6. 试求1030301的素因子标准分解式。

7. 试求e的连分数到第五位。

8. 在应用问题上(例如密码)，整数的因子分解有重要性。一般言之，理论上很简单的整数分解，实际做起来是很繁的，例如，试求 1234567891011121314151617 的素因子标准分解式。

9. n阶进位法：把实数的小数部分先用1/2度量之，所余用1/3！度量之，依此反复类推。换句话说，如$0\leqslant a<1$，则将a表作：

$$a=\frac{a_2}{2!}+\frac{a_3}{3!}+\cdots+\frac{a_n}{n!}+\cdots,\qquad 0\leqslant a_n<n,$$

其中a_n为整数。证明：如果a是有理数，那么只有有限个a_n不为零。

10. 利用题 9 证明 e 是无理数。

11. 埃及记数法：证明每个眞分数a ($0<a<1$) 可以写成$\sum\frac{1}{r_i}$的有限和形式，其中r_i两两不同，且为正整数。

12. 设x是一个实数，令

$$((x))=\begin{cases}x-[x]-1/2; & \text{当 } x \text{ 不是整数，}\\ 0; & \text{当 } x \text{ 是整数。}\end{cases}$$

证明：

$$\sum_{r=1}^{k}\left(\left(\frac{r}{k}\right)\right)=0.$$

13. 令 h,k 为整数，定义

$$s(h,k)=\sum_{r=1}^{k-1}\frac{r}{k}\left(\frac{hr}{k}-\left[\frac{hr}{k}\right]-\frac{1}{2}\right).$$

证明：

(1) $s(h,k)=\sum_{r=1}^{k-1}\left(\left(\frac{r}{k}\right)\right)\left(\left(\frac{hr}{k}\right)\right).$

(2) 如果 $h>0$，$k>0$，$(h,k)=1$，则有
$12hks(h,k)+12khs(k,h)=h^2+k^2-3hk+1.$

§3 同余式

定义1.12 设m为非零整数。两个整数 a,b 如果适合

$$m\mid a-b,$$

则称 a 与 b 对模 m **同余**，记为

$$a\equiv b\ (\mathrm{mod}\, m).$$

反之，如果a 与 b 对模m不同余时，则记为

$$a\not\equiv b\ (\mathrm{mod}\, m).$$

讨论 同余关系是一个等价关系。事实上，容易验证

1) 反身性：$a\equiv a\ (\mathrm{mod}\, m)$；

2) 对称性：如果 $a\equiv b\ (\mathrm{mod}\, m)$，则 $b\equiv a\ (\mathrm{mod}\, m)$；

3) 传递性：如果 $a\equiv b\ (\mathrm{mod}\, m)$，$b\equiv c\ (\mathrm{mod}\, m)$，则
$m\mid a-b,\quad m\mid b-c\Longrightarrow m\mid (a-b)+(b-c)=a-c,$
即 $a\equiv c\ (\mathrm{mod}\, m)$。

按照定义1.4*，同余关系把整数集 $\boldsymbol{Z}$ 划分成一些“同余子

集”.

定义1.13 称集合

$$\{b: b\equiv a(\bmod m)\}$$

为模 m 的**同余子集**，记为$[a]_m$。$\boldsymbol{Z}$对模m的同余关系的商集记为$\boldsymbol{Z}_m$. 如果 $b\in[a]_m$，且$0\leqslant b<|m|$，则称 b 为$[a]_m$的**主余数**.

引理 $\boldsymbol{Z}_m=\{[0]_m,[1]_m,[2]_m,\cdots,[|m|-1]_m\}$.

证明 任取一个同余子集$[a]_m$，按照欧几里得算法，存在整数 q 及 r，使得

$$a=q|m|+r,\qquad 0\leqslant r<|m|.$$

于是$[a]_m=[r]_m$。又如果 $0\leqslant i<j\leqslant|m|$时，显然有

$$[i]_m\neq[j]_m. \quad \blacksquare$$

从代数观点看来，$\boldsymbol{Z}_m$ 的重要性质是在其中可以定义 自然的加、减、乘法运算. 我们有如下的定理:

定理1.6 如果$[a]_m=[i]_m$，$[b]_m=[j]_m$，则有

$$[a+b]_m=[i+j]_m,\qquad [a-b]_m=[i-j]_m,$$

$$[ab]_m=[ij]_m.$$

于是我们可以定义

$$[i]_m+[j]_m=[i+j]_m,\qquad [i]_m-[j]_m=[i-j]_m,$$

$$[i]_m[j]_m=[ij]_m.$$

这些运算适合如下的法则:

1) **结合律**: $([i]_m+[j]_m)+[k]_m=[i+j+k]_m$
$=[i]_m+([j]_m+[k]_m)$,
$([i]_m[j]_m)[k]_m=[ijk]_m=[i]_m([j]_m[k]_m)$;

2) **交换律**: $[i]_m+[j]_m=[j]_m+[i]_m$,
$[i]_m[j]_m=[j]_m[i]_m$;

3) **分配律**: $[i]_m([j]_m+[k]_m)=[i]_m[j]_m+[i]_m[k]_m$;

4) **有幺元**: $[0]_m$是加法的幺元，即$[0]_m+[i]_m=[i]_m$，$[1]_m$是乘法的幺元，即$[1]_m[i]_m=[i]_m$;

5) 有加法**逆元**: $[-i]_m$是$[i]_m$的加法逆元，即

$$[-i]_m+[i]_m=[0]_m.$$

证明 如上，设$[a]_m=[i]_m$，$[b]_m=[j]_m$，则有

$$m\,|\,a-i,\qquad m\,|\,b-j.$$

故有$m\,|\,(a-i)+(b-j)=(a+b)-(i+j)$，即

$$a+b\equiv i+j(\mathrm{mod}\ m),$$

也即
$$[a+b]_m=[i+j]_m.$$

同法可证 $[a-b]_m=[i-j]_m$. 又知

$$m\,|\,b(a-i)+i(b-j)=ab-ij,$$

故 $ab\equiv ij(\mathrm{mod}\ m)$，即有$[ab]_m=[ij]_m$.

应用上面的结果，我们有

$$[a]_m+[b]_m=[a+b]_m=[i+j]_m=[i]_m+[j]_m.$$

因此，同余子集加法的结果是唯一确定的，与同余子集$[a]_m$，$[b]_m$的不同表示方法无关。通常，如果从运算或映射的定义可以推知结果的唯一性，则称此定义是良好的，亦即是可以成立的。上面已证明了同余子集加法的定义是良好的，类似地可证减法与乘法的定义也皆是良好的。至于定理中的五项运算法则是简明易证的，请读者自证之。▌

例3 令$m=2$。$\boldsymbol{Z}_2=\{[0]_2,[1]_2\}$，其中$[0]_2$为偶数集，$[1]_2$为奇数集。$[0]_2+[0]_2=[0]_2$，$[0]_2+[1]_2=[1]_2$，$[1]_2+[1]_2=[0]_2$，即偶＋偶＝偶，偶＋奇＝奇，奇＋奇＝偶。

令$m=3$。易知$[10]_3=[1]_3$，$[10^n]_3=([10]_3)^n=([1]_3)^n=[1^n]_3=[1]_3$。由此立得十进位整数$n_sn_{s-1}\cdots n_2n_1$满足等式

$$[n_sn_{s-1}\cdots n_2n_1]_3=[n_1+n_2+\cdots+n_s]_3.$$

例如，$[741]_3=[12]_3=[3]_3=[0]_3$，故$3\,|\,741$。

令$m=11$，易知$[10]_{11}=[-1]_{11}$，$[10^n]_{11}=[(-1)^n]_{11}$。所以十进位整数满足

$$[n_sn_{s-1}\cdots n_2n_1]_{11}=\left[\sum_{i=1}^{s}(-1)^{i-1}n_i\right]_{11}.$$

例如，$[5678]_{11}=[-5+6-7+8]_{11}=[2]_{11}$，即5678除以11余2。

例 4　循环赛的赛程．设有偶数个队：队1、队2、…、队 $2n$ 举行循环赛(如实际上是奇数个队，则不妨用一空牌充作一个队，使队数为偶数)，两两成对拼搏．设同时进行 n 场比赛，问题在于如何安排整个赛程．以下用同余式提供一个简明的赛程．

令 $m=2n-1$．规定在进行第 i 次比赛时，队 a 根据下面的同余式，解出 b 来，然后去找 b 队比赛：

$$b\equiv i-a(\mathrm{mod}\ m),$$

此处 a 和 b 受 $1\leqslant a,b\leqslant m$ 的限制，而且如果 $b=a$ 时，则队 a 去找队 $2n$ 比赛．

要说明上述的办法是合理的，必须证明下面三点：1）如队 a 找队 b 比赛时，队 b 必然找队 a；2）每次必然有而且仅有一个队找队 $2n$ 比赛；3）当 i 自 1 到 $m=2n-1$ 变动时，队 a 的对手必须都不一样．

因 $b\equiv i-a(\mathrm{mod}\ m)\Longrightarrow a\equiv i-b(\mathrm{mod}\ m)$，故 1）得证．因为除掉队 $2n$ 之后，剩下有奇数个队，所以这些队两两搭配后，必剩下某个队去找队 $2n$．我们说明这样的队只有一个．设队 a_1 及队 a_2 都找队 $2n$，则

$$a_1\equiv i-a_1(\mathrm{mod}\ m),\quad a_2\equiv i-a_2(\mathrm{mod}\ m).$$

故

$$2(a_1-a_2)\equiv 0(\mathrm{mod}\ m),$$

即 $m|2(a_1-a_2)$．但 m 为奇数，所以 $m|a_1-a_2$，即

$$a_1\equiv a_2(\mathrm{mod}\ m).$$

注意到 $1\leqslant a_1,a_2\leqslant m$，即知 $a_1=a_2$．故 2)得证．

仿上，读者试自证 3)．

定义1.14　称 $\boldsymbol{Z}_m$ 的子集 $\{[a]_m$：a 与 m 互素$\}$ 为模 m 的**缩剩余集**，记为 $\boldsymbol{Z}_m^*$．其基数称为**尤拉 φ 函数** $\varphi(m)$．

定理1.7（尤拉定理）　设 a 与 m 互素，则有

$$a^{\varphi(m)}\equiv 1(\mathrm{mod}\ m).$$

证明　考虑映射

$$\alpha: \boldsymbol{Z}_m^* \rightarrow \boldsymbol{Z}_m^*,$$

$$[b]_m \mapsto [ab]_m.$$

易知 α 为单射。事实上，如果$\alpha[b_1]_m = \alpha[b_2]_m$，则

$$[ab_1]_m = [ab_2]_m, \quad a(b_1 - b_2) \equiv 0 \pmod{m},$$

即

$$m \mid a(b_1 - b_2).$$

由于m与a互素，所以$m \mid b_1 - b_2$，即$[b_1]_m = [b_2]_m$，故α为单射。根据鸽笼定理，即知 α 为单满映射。于是有

$$\prod_{[b_i]_m \in Z_m^*} [b_i]_m = \prod_{[b_i]_m \in Z_m^*} [ab_i]_m,$$

即

$$\prod (ab_i) \equiv \prod b_i \pmod{m},$$

$$(a^{\varphi(m)} - 1) \prod b_i \equiv 0 \pmod{m},$$

$$m \mid (a^{\varphi(m)} - 1) \prod b_i.$$

而b_i皆与m互素，故$m \mid (a^{\varphi(m)} - 1)$，即$a^{\varphi(m)} \equiv 1 \pmod{m}$。▌

极易从尤拉定理导出下面的定理。

定理1.8（费马定理） 设 p 为素数，$p \nmid a$，则有

$$a^{p-1} \equiv 1 \pmod{p}.$$

证明 在尤拉定理中令$m = p$，不难看出$\varphi(p) = p - 1$。▌

系 设 p 为素数，a 为任意数，则总有

$$a^p \equiv a \pmod{p}. ▌$$

例 5 应用费马定理，可编一种简易而极难破解的密码如下：

1）任何文词皆可写成电码，这就是所谓"明码"。电码都是数字。对文词的长度可加以限制（长文可分段送出）。简言之，我们仅考虑小于某正整数N的正整数。

2）取一素数 p，使$p > N$。再取另一整数 q，使 q 与$p-1$互素，并与 p 的大小相仿。

3）令$m = pq$。公布m，把因数分解 $m = pq$ 当成绝密，不令人知。

4）设有一明码 $n < N$。解

$$n^m \equiv c(\bmod m), \quad 1 \leqslant c < m,$$

得c，此即讯息n的密码。请注意$c \neq 0$。

5) 收码人知道因数分解$m = pq$，而且已知q与$p-1$互素，于是得二整数a, b，使$aq - b(p-1) = 1$，即$aq = 1 + b(p-1)$。所以收得密码c以后，立即进行下列对模p的运算：

$$c^a \equiv n(\bmod p), \quad 1 \leqslant n < p,$$

（这是因为$c^a \equiv (n^{pq})^a \equiv (n^{aq})^p \equiv (n^{1+b(p-1)})^p \equiv n^p(n^{p-1})^{bp} \equiv n^p 1^{bp} \equiv n^p \equiv n(\bmod p)$），即解得$n$。

在上面的过程中，显然需要一台电子计算机进行运算。这个密码的要点是两个速度的比较：一是3)中求一已知数m的因数分解，二是4)及5)中求高次方的余数。以目前的技术水平来看，“一”是极缓慢的过程，而“二”是极为便捷的。这就是这种密码的成功之处。

定理1.9（威尔逊定理） 设p为素数，则

$$(p-1)! \equiv -1(\bmod p).$$

证明 我们先说明对于任一整数i $(1 \leqslant i \leqslant p-1)$，$[i]_p$都有乘法逆元素，并且此逆元素唯一，即有唯一的$[a]_p$，使

$$[a]_p[i]_p = [1]_p.$$

事实上，由于$1 \leqslant i \leqslant p-1$，故$i$与$p$互素，故有整数$a, b$，使得

$$ai + bp = 1,$$

即有$[a]_p[i]_p = [1]_p$。如果又有$[c]_p$，使$[c]_p[i]_p = [1]_p$，则

$$[a]_p[i]_p - [c]_p[i]_p = [a-c]_p[i]_p = [0]_p,$$

故$p \mid (a-c)i$。但i, p互素，所以$p \mid (a-c)$，即有$[a]_p = [c]_p$。

欲证$(p-1)! \equiv -1(\bmod p)$，只要证

$$\prod_{i=1}^{p-1} [i]_p = [-1]_p.$$

对某个$i(1 \leqslant i \leqslant p-1)$，如果$[i]_p$与其逆元素不同，则可与其逆元素相乘得出$[1]_m$。于是在上面的乘式中只剩下与其逆元素相同的$[i]_p$的乘积。而$[i]_p$与其逆元素相同的充要条件是

$$[i]_p^2=[1]_p,\qquad [i]_p^2-[1]_p^2=[0]_p,$$

$$[(i-1)(i+1)]_p=[0]_p,$$

即 $p|i-1$ 或 $p|i+1$，亦即 $i=1$ 或 $i=p-1$。于是有

$$\prod_{i=1}^{p-1}[i]_p=[1]_p[p-1]_p=[-1]_p. \quad \blacksquare$$

习　题

1．设 m,n 是两个正整数，d 是它们的最大公因子，d 中互不相同素因子之积记为 p。证明：

$$\frac{\varphi(mn)}{\varphi(m)\varphi(n)}=\frac{p}{\varphi(p)}.$$

2．设 p 为奇素数，证明：

$$\left[\left(\frac{p-1}{2}\right)!\right]^2\equiv(-1)^{(p+1)/2}(\bmod p).$$

3．设 m 是一正整数。在 $\mathbf{Z}_m$ 中找出所有满足如下条件的子集 S：

(1) 若 $[a]_m,[b]_m\in S$，则 $[a]_m+[b]_m\in S$；

(2) 若 $[a]_m\in S$，则对一切 $[b]_m$，有 $[a]_m[b]_m\in S$。

4．设 m 为正整数，$a,b\in\mathbf{Z}$，d 是 m,a 的最大公因子，$d|b$。证明同余式方程

$$ax+b\equiv 0(\bmod m)$$

恰有 d 个解满足 $0\leqslant x<m$。

5．空间取 n 个点，两两用有颜色的线相连，使对任给的点而言，连接此点的线的颜色均不相同。证明：只要有 n 种不同颜色的线，便足以完成上面的任务。

6．证明：如整数 x,y,z 适合 $x^2+y^2=z^2$，则 $3|xyz$。

7．设 $p=2,3,5$，试写出二项式系数 $\binom{n}{i}(\bmod p)$，其中 $1\leqslant n\leqslant 10$。

8. 设 p 为素数，求 $\varphi(p^n)$。

9. 证明对整数 x 有 $(1\pm x)^p \equiv 1\pm x^p \pmod p$。

10. 设正整数 m 的素因子标准分解式为 $m=p_1^{l_1}p_2^{l_2}\cdots p_s^{l_s}$，试求 $\varphi(m)$。

§4 中国剩余定理

中国剩余定理源出于三国或晋时的古数学书《孙子算经》。其中有一题："今有物不知其数。三三数之剩二，五五数之剩三，七七数之剩二，问物几何？"以同余写出，即求 x，使

$$x\equiv 2 \pmod 3),\quad x\equiv 3 \pmod 5,\quad x\equiv 2 \pmod 7.$$

《孙子算经》中给出答案 $x=23$.原来的解法传至今世.后世的数学家迭加研究类似的问题.唐僧一行、李淳风等卓具贡献.宋代数学家秦九韶(1247年)是集其大成者。

联立的一元一次同余式，后世称之为"大衍"，其解法称为"大衍求一"。以原题为例，可以化为三组联立同余式：

$$\begin{cases} x_1\equiv 1 \pmod 3, \\ x_1\equiv 0 \pmod 5, \\ x_1\equiv 0 \pmod 7, \end{cases}\quad \begin{cases} x_2\equiv 0 \pmod 3, \\ x_2\equiv 1 \pmod 5, \\ x_2\equiv 0 \pmod 7, \end{cases}\quad \begin{cases} x_3\equiv 0 \pmod 3, \\ x_3\equiv 0 \pmod 5, \\ x_3\equiv 1 \pmod 7. \end{cases}$$

不难解得 $x_1=70$，$x_2=21$，$x_3=15$。令

$$x=2x_1+3x_2+2x_3=223,$$

即为原题的一解。又易看出

$$x=233\pm n\cdot 3\cdot 5\cdot 7=223\pm 105n \quad (n\text{为非负整数})$$

皆为原题的解。$[233]_{105}$ 的主余数，即 23，自然是原题的最小正整数解。

对于此题，又有如下之歌诀(程大位：《算法统宗》(1593年))。

"三人同行七十稀，五树梅花廿一枝，

七子团圆正半月，除百零五便得知。"

中国剩余定理又称"孙子定理"。

现在我们用同余式，证明中国剩余定理。

定理1.10（中国剩余定理） 设整数 $m_1, m_2, \cdots, m_n$ 两两互素。令 $m = \prod_{i=1}^{n} m_i$ 。则对于任意的 j（$1 \leqslant j \leqslant n$），下列的联立同余式有解：

$$\begin{cases} x_j \equiv 1 \pmod{m_j}, \\ x_j \equiv 0 \pmod{m_i}, \quad i \neq j. \end{cases}$$

令 $x = \sum_{j=1}^{n} a_j x_j$，则 x 适合下列的联立同余式

$$x \equiv a_j \pmod{m_j}, \quad j = 1, 2, \cdots, n.$$

上列联立同余式的解即$[x]_m$，于是其最小非负整数解是 x 对模 m 的主余数。

证明 1）根据已知条件，$m_1, m_2, \cdots, m_n$ 两两互素，即无素数作为公因数，于是 m_j 与 $\prod_{i \neq j} m_i$ 必互素，即最大公因数为 1。根据定理1.4，必有整数 a, b，使得 $am_j + b\prod_{i \neq j} m_i = 1$。令

$$x_j = 1 - am_j = b\prod_{i \neq j} m_i,$$

则显然有

$$x_j \equiv 1 \pmod{m_j}, \quad x_j = 0 \pmod{m_i}, \quad i \neq j.$$

2）因$x = \sum_{j=1}^{n} a_j x_j$，故

$$[x]_{m_i} = \left[\sum_{j=1}^{n} a_j x_j\right]_{m_i} = \sum_{j=1}^{n} [a_j x_j]_{m_i} = [a_i]_{m_i},$$

即 $x \equiv a_i \pmod{m_i}$，$i = 1, 2, \cdots, n$。

3）设 y 也适合此联立同余式，则有

$$y \equiv a_i \pmod{m_i}, \quad i = 1, 2, \cdots, n.$$

$$x - y \equiv 0 \pmod{m_i}, \quad m_i \mid x - y.$$

因$m_1, m_2, \cdots, m_n$两两互素，故得

$$m=\prod_{i=1}^{n} m_i \mid x-y, \qquad x\equiv y(\text{mod } m).$$

反之，易于看出$[x]_m$的任意元素皆适合此联立同余式。▎

中国剩余定理又可表述为映射的某种性质。我们有

定理1.11 设 $m_1, m_2, \cdots, m_n$ 为两两互素的整数。我们令 $m=\prod_{i=1}^{n} m_i$。令 $\varphi: \boldsymbol{Z}_m \to \prod_{i=1}^{n} \boldsymbol{Z}_{m_i}$ 为从 $\boldsymbol{Z}_m$ 到直积 $\prod_{i=1}^{n} \boldsymbol{Z}_{m_i}$ 的映射，其定义如下：

$$\varphi([a]_m)=([a]_{m_1}, [a]_{m_2}, \cdots, [a]_{m_n}),$$

则 φ 为单满映射。

证明 已知 $\boldsymbol{Z}_m$ 的基数是$|m|$，$\prod_{i=1}^{n} \boldsymbol{Z}_{m_i}$的基数是$\prod_{i=1}^{n}|m_i|$，故二者相等。根据鸽笼定理，仅须证明 φ 是满射便足够了。

令$([a_1]_{m_1},[a_2]_{m_2},\cdots,[a_n]_{m_n})$ 为$\prod_{i=1}^{n} \boldsymbol{Z}_{m_i}$的任一元素。根据中国剩余定理，下列的联立同余式有解 x：

$$x\equiv a_i(\text{mod } m_i), \qquad i=1,2,\cdots,n.$$

则有$[x]_{m_i}=[a_i]_{m_i}$。于是

$$\begin{aligned}\varphi([x]_m)&=([x]_{m_1},[x]_{m_2},\cdots,[x]_{m_n})\\&=([a_1]_{m_1},[a_2]_{m_2},\cdots,[a_n]_{m_n}),\end{aligned}$$

即 φ 为满射。▎

讨论 也很容易从定理1.11导出定理1.10。设已知定理1.11是正确的，求解联立同余式

$$x\equiv a_i(\text{mod } m_i).$$

根据定理1.11，有一 a，使得

$$[a]_{m_i}=[a_i]_{m_i}.$$

显然，$x=a$ 即是欲求的解。所以，定理 1.10 和定理 1.11 是等同的。

习　题

1. 七数剩一，八数剩二，九数剩三，问本数(即求最小的正整数解)。参看杨辉“续古摘奇算法”(1275年)。

2. 设m_1, m_2为正整数，其最大公因子与最小公倍数分别为d, m，又设$a_1, a_2 \in \boldsymbol{Z}$。证明：若$d \mid (a_1-a_2)$，则同余式组

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \end{cases}$$

在$0 \leqslant x < m$内有唯一解。

3. 在集合$\boldsymbol{Z}_2$与$\boldsymbol{Z}_3$的直积$\boldsymbol{Z}_2 \times \boldsymbol{Z}_3$内定义加法、乘法如下：

$$([a]_2, [b]_3) + ([a']_2, [b']_3) = ([a]_2 + [a']_2, [b]_3 + [b']_3),$$
$$([a]_2, [b]_3)([a']_2, [b']_3) = ([a]_2[a']_2, [b]_3[b']_3).$$

证明定理1.11中所定义的$\boldsymbol{Z}_6$到$\boldsymbol{Z}_2 \times \boldsymbol{Z}_3$的映射$\varphi$满足：

$$\varphi([a]_6 + [b]_6) = \varphi([a]_6) + \varphi([b]_6),$$
$$\varphi([a]_6[b]_6) = \varphi([a]_6)\varphi([b]_6).$$

4. 大衍求一术与Lagrange内插法的关系：假设$\boldsymbol{Q}[x], \boldsymbol{R}[x]$分别代表有理系数与实系数多项式所成的集合，试仿照大衍求一术在$\boldsymbol{Q}[x]$或$\boldsymbol{R}[x]$内求解下列同余式：

$$f(x) \equiv a_i \pmod{(x-b_i)} \quad (i=1,2,\cdots,n),$$

此处$a_i, x-b_i \in \boldsymbol{Q}[x]$(或$\boldsymbol{R}[x]$)，而且$b_1, \cdots, b_n$互不相同。

提示：证明所寻求的解为 Lagrange 内插多项式

$$f(x) = \sum_{j=1}^{n} a_j \prod_{\substack{i=1 \\ i \neq j}}^{n} \frac{(x-b_i)}{(b_j-b_i)}.$$

5. 试求一次数最小的有理系数多项式$f(x)$，使它满足如下联立同余式：

$$\begin{cases} f(x)\equiv 1(\bmod x), \\ f(x)\equiv 1(\bmod(x+1)), \\ f(x)\equiv 3(\bmod(x-1)). \end{cases}$$

6. 设$m_1,\cdots,m_k$是正整数，定义$\boldsymbol{Z}$到$\boldsymbol{Z}_{m_1}\times\cdots\times\boldsymbol{Z}_{m_k}$的映射如下：

$$\varphi(x)=([x]_{m_1},\cdots,[x]_{m_k})\quad(x\in\boldsymbol{Z}),$$

试证明：φ是满射$\Longleftrightarrow(m_i,m_j)=(1)(\forall i\neq j)$。当$\varphi$是满射时，试求$(0,\cdots,0)$的全体原象(其中0表示$\boldsymbol{Z}_{m_i}$中的$[0]_{m_i}$)。

§5 复整数集

令

$$\boldsymbol{Z}[\mathrm{i}]=\boldsymbol{Z}+\boldsymbol{Z}\mathrm{i}=\{a+b\mathrm{i}:\ a,b\in\boldsymbol{Z}\},$$

其中$\mathrm{i}=\sqrt{-1}$。$\boldsymbol{Z}[\mathrm{i}]$即**复整数集**，也称**高斯整数集**。复整数集$\boldsymbol{Z}[\mathrm{i}]$可以理解成复数平面上的网格点集。不难看出在$\boldsymbol{Z}[\mathrm{i}]$中可以进行加、减、乘运算，如同整数集那样。

我们将像对整数集做过的那样，证明复整数集$\boldsymbol{Z}[\mathrm{i}]$的“唯一分解定理”。复整数集$\boldsymbol{Z}[\mathrm{i}]$是更广泛的“代数整数环”的一个特例。代数整数环是“代数数论”的题材。

定义1.15 一个复整数$a+b\mathrm{i}\in\boldsymbol{Z}[\mathrm{i}]$的**范数**$\mathrm{N}(a+b\mathrm{i})$的定义为

$$\mathrm{N}(a+b\mathrm{i})=a^2+b^2.$$

讨论 不难看出，$\mathrm{N}(a+b\mathrm{i})$是复数平面上自原点O到点$a+b\mathrm{i}$的距离的平方。

定理1.12(欧几里得算法) 设$\delta=d_1+d_2\mathrm{i}$为$\boldsymbol{Z}[\mathrm{i}]$中任意不为零的元素，$\alpha=a_1+a_2\mathrm{i}$为$\boldsymbol{Z}[\mathrm{i}]$的任意元素。则必有$\beta=b_1+b_2\mathrm{i}$，$\gamma=r_1+r_2\mathrm{i}\in\boldsymbol{Z}[\mathrm{i}]$，使得

$$\alpha=\beta\delta+\gamma,\quad 0\leqslant N(\gamma)<N(\delta).$$

证明 1) 几何证法。令

$$L=\{(c_1+c_2\mathrm{i})\delta:\ c_1+c_2\mathrm{i}\in \boldsymbol{Z}[\mathrm{i}]\}.$$

不难看出，L 即图 1.1 所示的网格点集。显然，$\alpha=a_1+a_2\mathrm{i}$ 必落

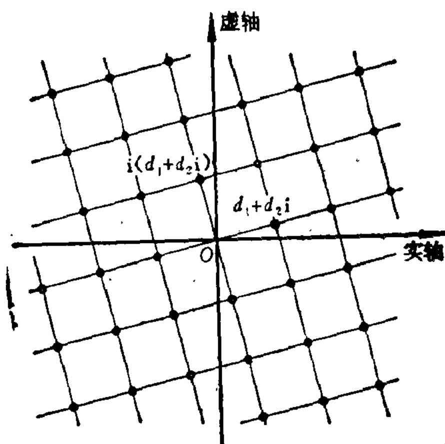


图 1.1

在某网格中。组成网格的正方形的边长为$\sqrt{N(\delta)}$，于是必然有某网格点 $\beta\delta$ 与 α 的距离小于$\sqrt{N(\delta)}$，即

$$\sqrt{N(\alpha-\beta\delta)}<\sqrt{N(\delta)},\qquad N(\alpha-\beta\delta)<N(\delta).$$

令$\gamma=\alpha-\beta\delta$，即得本定理。

2) 代数证法。把上述证法代数化，可以得到不需要借助于图形的代数证法如下：考虑

$$\frac{\alpha}{\delta}=\frac{a_1+a_2\mathrm{i}}{d_1+d_2\mathrm{i}}=\frac{a_1d_1+a_2d_2}{d_1^2+d_2^2}+\frac{a_2d_1-a_1d_2}{d_1^2+d_2^2}\mathrm{i},$$

用下法，直接求出 $\beta=b_1+b_2\mathrm{i}$。令b_1 为最接近$\dfrac{a_1d_1+a_2d_2}{d_1^2+d_2^2}$的整数，

b_2为最接近$\dfrac{a_2d_1-a_1d_2}{d_1^2+d_2^2}$的整数，即

$$\left|\frac{a_1d_1+a_2d_2}{d_1^2+d_2^2}-b_1\right|\leqslant\frac{1}{2},\qquad\left|\frac{a_2d_1-a_1d_2}{d_1^2+d_2^2}-b_2\right|\leqslant\frac{1}{2}.$$

令

$$\gamma=\alpha-\beta\delta=\delta\left(\frac{\alpha}{\delta}-\beta\right)=(d_1+d_2\mathrm{i})(\varepsilon_1+\varepsilon_2\mathrm{i})$$
$$=(d_1\varepsilon_1-d_2\varepsilon_2)+(d_2\varepsilon_1+d_1\varepsilon_2)\mathrm{i}=r_1+r_2\mathrm{i},$$

其中$|\varepsilon_1|\leqslant1/2$，$|\varepsilon_2|\leqslant1/2$。于是

$$\mathrm{N}(\gamma)^2=(d_1\varepsilon_1-d_2\varepsilon_2)^2+(d_2\varepsilon_1+d_1\varepsilon_2)^2$$
$$=d_1^2\varepsilon_1^2+d_1^2\varepsilon_2^2+d_2^2\varepsilon_2^2+d_2^2\varepsilon_1^2$$
$$<d_1^2+d_2^2=\mathrm{N}(\delta)^2.\quad \blacksquare$$

讨论 从上面的几何证法中不难看出，β,γ有时可能有四组不同的值，所以β,γ不是唯一的。

定理1.13 $\mathrm{N}((a_1+a_2\mathrm{i})(b_1+b_2\mathrm{i}))=\mathrm{N}(a_1+a_2\mathrm{i})\mathrm{N}(b_1+b_2\mathrm{i})$。

证明 $\mathrm{N}((a_1+a_2\mathrm{i})(b_1+b_2\mathrm{i}))$

$$=\mathrm{N}((a_1b_1-a_2b_2)+(a_1b_2+a_2b_1)\mathrm{i})$$
$$=(a_1b_1-a_2b_2)^2+(a_1b_2+a_2b_1)^2$$
$$=a_1^2b_1^2+a_2^2b_2^2+a_1^2b_2^2+a_2^2b_1^2$$
$$=(a_1^2+a_2^2)(b_1^2+b_2^2)$$
$$=\mathrm{N}(a_1+a_2\mathrm{i})\mathrm{N}(b_1+b_2\mathrm{i}).\quad \blacksquare$$

在整数集$\mathbf{Z}$中，仅只1和-1有乘法的逆元素，即$1^{-1},(-1)^{-1}$也是整数。在复整数集中，有乘法逆元素的数是较多的。且看下面的定理。

定理1.14 一个复整数$a_1+a_2\mathrm{i}$有乘法逆元素——即存在复整数$b_1+b_2\mathrm{i}$，使$(b_1+b_2\mathrm{i})(a_1+a_2\mathrm{i})=1$——的充要条件是$\mathrm{N}(a_1+a_2\mathrm{i})=1$。于是这样的$a_1+a_2\mathrm{i}$必为$\pm1,\pm\mathrm{i}$之一。

证明 充分性。 $(a_1-a_2\mathrm{i})(a_1+a_2\mathrm{i})=\mathrm{N}(a_1+a_2\mathrm{i})=1$，即

$a_1+a_2\mathrm{i}$ 有逆元素 $a_1-a_2\mathrm{i}$。

必要性。由于

$$\mathrm{N}(b_1+b_2\mathrm{i})\mathrm{N}(a_1+a_2\mathrm{i})=\mathrm{N}((b_1+b_2\mathrm{i})(a_1+a_2\mathrm{i}))$$
$$=\mathrm{N}(1)=1,$$

而 $\mathrm{N}(b_1+b_2\mathrm{i})$，$\mathrm{N}(a_1+a_2\mathrm{i})$ 皆为非负整数，故

$$\mathrm{N}(b_1+b_2\mathrm{i})=\mathrm{N}(a_1+a_2\mathrm{i})=1. \quad \blacksquare$$

定义1.16 设$\alpha,\beta,\gamma\in\boldsymbol{Z}[\mathrm{i}]$，如果$\alpha=\beta\gamma$，则称$\alpha$为$\beta$的**倍数**，$\beta$是$\alpha$的**因数**，用符号$\beta|\alpha$表示之。如果 $\beta|\alpha_1,\beta|\alpha_2,\cdots,\beta|\alpha_n$（这里$\alpha_1,\alpha_2,\cdots,\alpha_n$都是复整数），则称$\beta$是$\alpha_1,\alpha_2,\cdots,\alpha_n$ 的**公因数**。如果β是$\alpha_1,\alpha_2,\cdots,\alpha_n$的公因数，而且是$\alpha_1,\alpha_2,\cdots,\alpha_n$ 的任意公因数β'的倍数，则称β为$\alpha_1,\alpha_2,\cdots,\alpha_n$的**最大公因数**。

定理1.15 设$\alpha_1,\alpha_2,\cdots,\alpha_n\in\boldsymbol{Z}[\mathrm{i}]$。令

$$(\alpha_1,\alpha_2,\cdots,\alpha_n)$$
$$=\left\{\sum_{j=1}^{n}\beta_j\alpha_j:\ \beta_j\in\boldsymbol{Z}[\mathrm{i}],\ \forall\, j=1,2,\cdots,n\right\}.$$

则

1）存在 $\delta\in\boldsymbol{Z}[\mathrm{i}]$，使得$(\alpha_1,\alpha_2,\cdots,\alpha_n)=(\delta)$；

2）如果$(\alpha_1,\alpha_2,\cdots,\alpha_n)=(\delta),\delta\neq0$，则$\delta$ 是 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 的一个最大公因数；

3）如果$(\delta)=(\delta')$，则$\delta=\varepsilon\delta'$，其中$\varepsilon$为$\pm1,\pm\mathrm{i}$之一。

证明 1）先证明$n=2$时，$(\alpha_1,\alpha_2)=(\delta_1)$。令 δ_1 为(α_1,α_2)中有最小正范数 $\mathrm{N}(\delta_1)$ 者。如果不存在这样的 δ_1，则(α_1,α_2) 中的复整数的范数皆为零，即$(\alpha_1,\alpha_2)=(0)$，可取 $\delta=0$。因此只须考虑存在上述的δ_1的情形。按照欧几里得算法，存在复整数β_1,γ_1，使得

$$\alpha_1=\beta_1\delta_1+\gamma_1,\quad \mathrm{N}(\gamma_1)<\mathrm{N}(\delta_1).$$

显然，$\gamma_1=\alpha_1-\beta_1\delta_1\in(\alpha_1,\alpha_2)$，故必有$\mathrm{N}(\gamma_1)=0$，$\gamma_1=0$，即有

$$\alpha_1=\beta_1\delta_1,\quad \delta_1|\alpha_1.$$

同法可证

$$\alpha_2=\beta_2\delta_1,\quad \delta_1|\alpha_2.$$

于是有$(\alpha_1,\alpha_2)\subset(\delta_1)$。显然，又有 $(\alpha_1,\alpha_2)\supset(\delta_1)$。我们证出 $(\alpha_1,\alpha_2)=(\delta_1)$。不难看出

$$(\alpha_1,\alpha_2,\alpha_3,\cdots,\alpha_n)=(\delta_1,\alpha_3,\cdots,\alpha_n),$$

用数学归纳法，即知存在δ，使得

$$(\alpha_1,\alpha_2,\cdots,\alpha_n)=(\delta).$$

2）因为

$$\alpha_i\in(\alpha_1,\alpha_2,\cdots,\alpha_n)=(\delta)=\{\beta\delta:\ \beta\in \boldsymbol{Z}[\mathrm{i}]\},$$

所以 $\delta|\alpha_i(i=1,2,\cdots,n)$，即 δ 是 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 的公因数。

设δ'是$\alpha_1,\alpha_2,\cdots,\alpha_n$的公因数，即

$$\delta'|\alpha_1,\quad \delta'|\alpha_2,\quad \cdots,\quad \delta'|\alpha_n.$$

因为 $\delta\in(\alpha_1,\alpha_2,\cdots,\alpha_n)$，故

$$\delta=\beta_1\alpha_1+\beta_2\alpha_2+\cdots+\beta_n\alpha_n,\quad \beta_i\in\boldsymbol{Z}[\mathrm{i}](i=1,2,\cdots,n).$$

因此$\delta'|\delta$。

3）我们有$\delta=\varepsilon\delta'$，$\delta'=\varepsilon'\delta$，其中$\varepsilon,\varepsilon'\in\boldsymbol{Z}[\mathrm{i}]$，即有

$$\delta=\varepsilon\varepsilon'\delta.$$

如果$\delta=0$，则$\delta'=0$，可取$\varepsilon=1$。如果$\delta\neq0$，则有

$$\varepsilon\varepsilon'=1.$$

根据定理1.14，ε必为$\pm1,\pm\mathrm{i}$之一。▎

类似于整数集$\boldsymbol{Z}$的情形，我们引入“不可约复整数”及“复素数”的概念。此外，由于有较多的可逆数(参见定理1.14)，我们还需要二复整数“相伴”的概念。

定义1.17 设α为一非零、非可逆的复整数，即$\alpha\in\boldsymbol{Z}[\mathrm{i}]$，$\alpha\neq0,\pm1,\pm\mathrm{i}$。如在$\alpha$的任意分解式$\alpha=\beta\gamma(\beta,\gamma\in\boldsymbol{Z}[\mathrm{i}])$中，必有$\beta$或$\gamma$为可逆复整数，则称$\alpha$为一个**不可分解的复整数**(或称**不可约复整数**)。如果$\alpha|\beta\gamma$时，必有$\alpha|\beta$或$\alpha|\gamma$，则称α为一个**复素数**。设α和α'为两个复整数，如果$\alpha=\varepsilon\alpha'$，此处$\varepsilon$为$\pm1,\pm\mathrm{i}$之一，则称$\alpha,\alpha'$为**相伴**的复整数。

讨论 设α与α'相伴。如果α为不可约的，则α'也为不可约

的；如果α是复素数，则α'也是复素数。

引理 不可约的复整数皆是复素数；反之，复素数皆是不可约的。

证明 设α为不可约复整数。设$\alpha|\beta\gamma(\beta,\gamma\in \boldsymbol{Z}[\mathrm{i}])$。根据定理1.15，存在$\delta\in \boldsymbol{Z}[\mathrm{i}]$，使得

$$(\alpha,\beta)=(\delta).$$

令

$$\alpha=\varepsilon_1\delta,\quad \beta=\varepsilon_2\delta.$$

由于α是不可约的，故ε_1,δ中必有一个是可逆的。如果ε_1可逆，则

$$\delta=\alpha\varepsilon_1^{-1},\quad \beta=\varepsilon_2\delta=(\varepsilon_2\varepsilon_1^{-1})\alpha,$$

即$\alpha|\beta$。如果δ是可逆的，由于$(\delta)=(\alpha,\beta)$，故可设

$$\delta=\varepsilon_3\alpha+\varepsilon_4\beta,\quad \varepsilon_3,\varepsilon_4\in \boldsymbol{Z}[\mathrm{i}].$$

于是

$$1=\delta^{-1}\varepsilon_3\alpha+\delta^{-1}\varepsilon_4\beta,\quad \gamma=\left(\delta^{-1}\varepsilon_3\gamma+\delta^{-1}\varepsilon_4\frac{\beta\gamma}{\alpha}\right)\alpha.$$

注意到$\dfrac{\beta\gamma}{\alpha}\in \boldsymbol{Z}[\mathrm{i}]$，即知$\alpha|\gamma$。因此，$\alpha$为复素数。

反之，设α为复素数，$\alpha=\beta\gamma$，则有$\alpha|\beta$或$\alpha|\gamma$。不妨设$\alpha|\beta$，即有$\varepsilon\in \boldsymbol{Z}[\mathrm{i}]$，使得

$$\beta=\varepsilon\alpha.$$

故$\alpha=\beta\gamma=(\varepsilon\gamma)\alpha$。由于$\alpha\neq0$，所以

$$\varepsilon\gamma=1,$$

即γ为可逆元。所以α为不可约的。▌

现在我们可以证明复整数的“基本定理”了。

定理1.16(唯一分解定理) 设α为一非零、非可逆的复整数，则

1) α可以分解成复素数的连乘积，即存在复素数$\beta_1,\beta_2,\cdots,\beta_n$，使得$\alpha=\prod\limits_{i=1}^{n}\beta_i$；

2) 设

(＊) $$\alpha=\prod_{i=1}^{n}\beta_i=\prod_{j=1}^{m}\gamma_j,$$

其中β_i,γ_j皆为复素数。则重新排列$\gamma_1,\gamma_2,\cdots,\gamma_m$后，必有$\beta_i$和$\gamma_i$是相伴的。于是$n=m$。

证明 1) 设α是不可约的，则令$n=1$，$\beta_1=\alpha$。否则，对$N(\alpha)$作数学归纳法。令$\alpha=\delta_1\delta_2$，其中δ_1,δ_2都不是可逆的。由于

$$N(\alpha)=N(\delta_1)N(\delta_2),$$

而$N(\delta_1)>1$，$N(\delta_2)>1$，故$N(\delta_1)<N(\alpha)$，$N(\delta_2)<N(\alpha)$。由归纳法，δ_1,δ_2都可分解成复素数的连乘积，而$\alpha=\delta_1\delta_2$，故α也可分解成复素数的连乘积。

2) 在题设之下，有

$$\beta_1\Big|\prod_{j=1}^{m}\gamma_j=\gamma_1\left(\prod_{j=2}^{m}\gamma_j\right),$$

于是有

$$\beta_1|\gamma_1 \quad 或 \quad \beta_1\Big|\prod_{j=2}^{m}\gamma_j.$$

应用数学归纳法，易于看出必有一j，使$\beta_1|\gamma_j$。重新排列$\gamma_1,\gamma_2,\cdots,\gamma_m$后，不妨设此$\gamma_j$为$\gamma_1$，即

$$\beta_1|\gamma_1.$$

令$\gamma_1=\varepsilon_1\beta_1$。由于$\gamma_1$是不可约的，故$\varepsilon_1$必为可逆的。代入(＊)式，有

$$\beta_1\left(\prod_{i=2}^{n}\beta_i\right)=\gamma_1\left(\prod_{j=2}^{m}\gamma_j\right)=\varepsilon_1\beta_1\prod_{j=2}^{m}\gamma_j.$$

两边消去β_1，得

$$\prod_{i=2}^{n}\beta_i=(\varepsilon_1\gamma_2)\prod_{j=3}^{m}\gamma_j.$$

根据数学归纳法，得出β_2与$(\varepsilon_1\gamma_2)$相伴，β_i与γ_i相伴$(i=3,\cdots,n)$。自然，β_2与γ_2也是相伴的。▍

以下，我们要找出$\boldsymbol{Z}[i]$的复素数。我们有

引理 设$\alpha\in\boldsymbol{Z}[i]$。如果$N(\alpha)$是$\boldsymbol{Z}$中的素数，则$\alpha$为一复素

数。如果 β 是复素数，则 $\bar{\beta}$ 也是。

证明 显然α为不可约的。

设 $\bar{\beta}=\overline{b_1+b_2\mathrm{i}}=b_1-b_2\mathrm{i}=(c_1+c_2\mathrm{i})(d_1+d_2\mathrm{i})$，则

$$\beta=\bar{\bar{\beta}}=\overline{(c_1+c_2\mathrm{i})(d_1+d_2\mathrm{i})}=(c_1-c_2\mathrm{i})(d_1-d_2\mathrm{i}),$$

故 $\bar{\beta}$ 可约$\Longrightarrow\beta$可约。 ▍

我们首先研究$\boldsymbol{Z}$中的素数p在$\boldsymbol{Z}[\mathrm{i}]$中的因数分解。

2 的复素数分解式如下：

$$2=-\mathrm{i}(1+\mathrm{i})^2$$

($\mathrm{N}(1+\mathrm{i})=2$，故$1+\mathrm{i}$为复素数）。这是所谓的**分歧型**。

设素数 p 适合 $p\equiv3(\mathrm{mod}\ 4)$。如果$a_1+a_2\mathrm{i}$为复素数，使

$$p=(a_1+a_2\mathrm{i})(\cdots)\cdots(\cdots)$$

（上式中的$(\cdots)$皆为复素数），则有

$$a_1^2+a_2^2=\mathrm{N}(a_1+a_2\mathrm{i})\mid p^2.$$

于是 $a_1^2+a_2^2=p$ 或 p^2。由于 p 为奇数，故 a_1,a_2 必为一奇一偶，所以

$$a_1^2+a_2^2=(1+2n)^2+(2m)^2=1+4(n+n^2+m^2)\equiv1(\mathrm{mod}\ 4).$$

而 $p\equiv3(\mathrm{mod}\ 4)$，故 $a_1^2+a_2^2\neq p$，必有

$$(a_1+a_2\mathrm{i})(a_1-a_2\mathrm{i})=p^2.$$

此式左端是两个复素数的乘积，如果 p 为可约的，则右端分解出素因数的个数至少为 4 。由此知 p 必为复素数，其复素数分解式即为

$$p=p.$$

这是所谓的**惯性型**。

设素数$p\equiv1(\mathrm{mod}\ 4)$，则根据下面的定理1.17，可知

$$p=a_1^2+a_2^2=(a_1+a_2\mathrm{i})(a_1-a_2\mathrm{i}),$$

因此 $\mathrm{N}(a_1+a_2\mathrm{i})=\mathrm{N}(a_1-a_2\mathrm{i})=p$，即 $a_1+a_2\mathrm{i}$ 为复素数。所以上式即为 p 的复素数分解式。这是所谓的**分解型**。

定理1.17（高斯定理） 一个奇素数 p 适合 $p\equiv1(\mathrm{mod}\ 4)$的充

要条件是存在整数 a_1, a_2，使$p=a_1^2+a_2^2$。

证明 充分性。a_1, a_2 必为一奇一偶。于是

$$p=a_1^2+a_2^2=(1+2n)^2+(2m)^2\equiv 1(\mathrm{mod}\ 4).$$

以下分段证明必要性。

1) 先证有一$b\in \boldsymbol{Z}$，使得 $b^2\equiv -1(\mathrm{mod}\ p)$。根据定理 1.9，知

$$(1)\qquad (p-1)!=1\cdot 2\cdot\cdots\cdot(p-3)(p-2)(p-1)\equiv -1(\mathrm{mod}\ p).$$

显然

$$[i]_p=-[p-i]_p,\qquad i=1,2,\cdots,\frac{p-1}{2}.$$

故(1)式变为

$$\left(\frac{p-1}{2}\right)!(-1)^{2n}\left(\frac{p-1}{2}\right)!\equiv -1(\mathrm{mod}\ p),$$

其中 $n=\dfrac{p-1}{4}\in \boldsymbol{Z}$。令 $b=\left(\dfrac{p-1}{2}\right)!$，即得$b^2\equiv -1(\mathrm{mod}\ p)$。

2) 设 p 在 $\boldsymbol{Z}[\mathrm{i}]$中是可约的，即 $p=(a_1+a_2\mathrm{i})(b_1+b_2\mathrm{i})$，且

$$\mathrm{N}(a_1+a_2\mathrm{i})>1,\quad \mathrm{N}(b_1+b_2\mathrm{i})>1.$$

则

$$p^2=\mathrm{N}(p)=\mathrm{N}(a_1+a_2\mathrm{i})\mathrm{N}(b_1+b_2\mathrm{i})=(a_1^2+a_2^2)(b_1^2+b_2^2),$$

故必有 $p=a_1^2+a_2^2$。

3) 我们来证明 p 在$\boldsymbol{Z}[\mathrm{i}]$中不可能是不可约的。考虑

$$(p,b+\mathrm{i})=(\delta),$$

其中 b 如 1)所示，即 $b^2\equiv -1(\mathrm{mod}\ p)$，$\delta\in \boldsymbol{Z}[\mathrm{i}]$。则有

$$\delta\,|\,p.$$

若 p 在$\boldsymbol{Z}[\mathrm{i}]$中是不可约的，则 δ 必为可逆元或与 p 相伴。

假设 δ 是可逆的。我们有

$$\alpha p+\beta(b+\mathrm{i})=\delta,\quad \alpha,\beta\in \boldsymbol{Z}[\mathrm{i}].$$

于是

$$\delta^{-1}\alpha p+\delta^{-1}\beta(b+\mathrm{i})=1.$$

令 $\delta^{-1}\alpha=a_1+a_2\mathrm{i}$，$\delta^{-1}\beta=b_1+b_2\mathrm{i}$. 代入上式，则有

$$a_1p+a_2p\mathrm{i}+(b_1b-b_2)+(b_1+bb_2)\mathrm{i}=1,$$

亦即

$$(a_1p+b_1b-b_2)+(a_2p+b_1+bb_2)\mathrm{i}=1.$$

故

$$a_1p+b_1b-b_2=1,\quad a_2p+b_1+bb_2=0.$$

将上面两式对模 p 取同余，得

$$b_1b-b_2\equiv1(\mathrm{mod}\ p),\quad b_1\equiv-bb_2(\mathrm{mod}\ p).$$

由此立得

$$-b_2b^2-b_2\equiv1(\mathrm{mod}\ p).$$

然而根据1)，又有

$$-b_2(b^2+1)\equiv0(\mathrm{mod}\ p).$$

以上两式显然是矛盾的，故 δ 不是可逆的。

再设δ与 p 相伴，即有一可逆的复整数ε，使

$$\delta=\varepsilon p.$$

但 $\delta|b+\mathrm{i}$，故 $\varepsilon p|b+\mathrm{i}$，$p|\varepsilon^{-1}(b+\mathrm{i})$. 但 $p\nmid\varepsilon^{-1}$，故 $p|b+i$. 令

$$b+\mathrm{i}=p(c_1+c_2\mathrm{i}).$$

则有 $b=pc_1$，$1=pc_2$. 最后这个等式显然是不可能的. 故 δ 也不与 p 相伴. ▌

以上讨论素数 p 在复整数集 $\boldsymbol{Z}[\mathrm{i}]$中的分解时，我们分别了三种情形：分歧型、惯性型、分解型，并以此得出了一些复素数及与其相伴的复素数. 实际上并沒有其它复素数了. 证法如下：令 $d_1+d_2\mathrm{i}=\alpha$ 为任一复素数. 取 $\mathrm{N}(\alpha)$的素因数 p，则有

1) 如果$p=2$，则$2=(1+\mathrm{i})(1-\mathrm{i})|\alpha\bar{\alpha}$. 于是$(1+\mathrm{i})$与$\alpha$ 或 $\bar{\alpha}$ 相伴，即$(1-\mathrm{i})$与 $\bar{\alpha}$ 或 α 相伴；

2) 如果$p\equiv3(\mathrm{mod}\ 4)$，则 p 为复素数. 而$p|\alpha\bar{\alpha}$，故 p 与α 或 $\bar{\alpha}$相伴. 又$\bar{p}=p$与$\bar{\alpha}$或α相伴，故p必与α及$\bar{\alpha}$相伴；

3) 如果$p\equiv1(\mathrm{mod}\ 4)$，设$p$在 $\boldsymbol{Z}[\mathrm{i}]$中的分解式为

$$p=(a_1+a_2\mathrm{i})(a_1-a_2\mathrm{i}),$$

则$(a_1+a_2\mathrm{i})(a_1-a_2\mathrm{i})\mid\alpha\bar{\alpha}$。所以$(a_1+a_2\mathrm{i})$与$\alpha$或$\bar{\alpha}$相伴，即$(a_1-a_2\mathrm{i})$与$\bar{\alpha}$或$\alpha$相伴。

从以上的讨论中，我们知道任意复素数必与已经得出的复素数之一相伴。

习　题

1. 在$\boldsymbol{Z}[\mathrm{i}]$内将下列复整数分解为复素数方幂的乘积：

$$4+7\mathrm{i},\quad 3+4\mathrm{i},\quad 8+11\mathrm{i}.$$

2. 判断下列复整数中哪些是复素数：

$$4+5\mathrm{i},\quad 4-5\mathrm{i},\quad 7+\mathrm{i},\quad -2-3\mathrm{i},\quad 5+9\mathrm{i}.$$

3. 令$\alpha=5-13\mathrm{i}$，$\delta=-2+3\mathrm{i}$，试求$\beta,\gamma\in\boldsymbol{Z}[\mathrm{i}]$，使

$$\alpha=\beta\delta+\gamma,\quad 0\leqslant N(\gamma)<N(\delta).$$

4. 利用$\boldsymbol{Z}[\mathrm{i}]$内的欧几里得算法求$7+\mathrm{i}$和$5+9\mathrm{i}$的最大公因子。

5. 设$\alpha\in\boldsymbol{Z}[\mathrm{i}]$，证明$\alpha$是复素数的充要条件是不存在复整数$\beta\neq\pm1,\pm\mathrm{i}$，使$(\alpha)\subsetneqq(\beta)$。

6. 设$\alpha,\beta\in\boldsymbol{Z}[\mathrm{i}]$且$(\alpha,\beta)=\boldsymbol{Z}[\mathrm{i}]$。又任取$\gamma,\delta\in\boldsymbol{Z}[\mathrm{i}]$，证明存在$x\in\boldsymbol{Z}[\mathrm{i}]$，使

$$x-\gamma\in(\alpha),\quad x-\delta\in(\beta).$$

7. 设$\alpha=a+b\mathrm{i}(a,b\in\boldsymbol{Q})$是下列多项式的根：

$$f(x)=x^n+a_1x^{n-1}+\cdots+a_n\quad(a_k\in\boldsymbol{Z}[\mathrm{i}]).$$

证明α必为复整数。

8. 给定素数3,5,11,13，判断哪些在$\boldsymbol{Z}[\mathrm{i}]$内可分解，在可分解的情况下求其复素数分解式。

9. 给定复素数$\alpha=-2+\mathrm{i}$。在$\boldsymbol{Z}[\mathrm{i}]$内定义等价关系如下：

$$\alpha\sim\beta\iff\beta-\alpha\in(\alpha).$$

试证明$\boldsymbol{Z}[\mathrm{i}]$关于上述等价关系的商集的基数有限，并在每个商集中找出一个代表元素。

10．设 α 是一个复素数，证明$(\alpha)\cap Z\neq\{0\}$，而且其中每个整数都是某个固定素数的倍数。

11．在Z中任给素数p，令(p)表示 p 的整倍数所成的集合。证明在 $Z[i]$中必存在一个复素数α，使$(\alpha)\cap Z=(p)$，并问在何时这种α是唯一的？在α不唯一时，有几种可能的选择？

12．设 α 是一个复素数，又设 $f(x)$是系数在 $Z[i]$ 内的多项式：

$$f(x)=a_0+a_1x+\cdots+a_nx^n\quad(a_k\in Z[i]).$$

如果$\alpha_0,\alpha_1,\cdots,\alpha_n$是$n+1$个复整数，使$f(\alpha_k)\in(\alpha)$，$k=0,1,2,\cdots,n$，且 $\alpha_i-\alpha_j\overline{\in}(\alpha)(i\neq j)$。证明 $f(x)$的系数 $a_k\in(\alpha)$，$k=0,1,2,\cdots,n$。

§6　p-adic 数与赋值

怎样从有理数集 Q 构造实数集 R 呢？我们用绝对值定义一"距离" $D_\infty(a,b)=|a-b|$。通常的距离定义如下。

定义1.18　设 S 为一集合。S 上一非负实数值的二元函数 $D(a,b)(a,b\in S)$，如适合下列的条件，则称为**距离**：

1) $D(a,b)=0\Longleftrightarrow a=b$；

2) $D(a,b)=D(b,a)$；

3) **三角不等式**：$D(a,b)+D(b,c)\geqslant D(a,c)$。

不难看出 $D_\infty(a,b)$是一距离。有了这个距离以后，我们将证明有理数集 Q 的所有"极限"的集合即是实数集 R。然而，有理数集 Q 还有其它的距离。且看下面的定义。

定义1.19　设 $p\in Z$ 为一素数。设 $a\in Q$ 为一非零的有理数。令

$$a=p^l\frac{m}{n},\quad p\nmid m,\ p\nmid n,\ l,m,n\in Z.$$

则 l 自然是由 a 唯一确定的。定义 a 的 p **赋值**为

$$v_p(a)=p^{-l},$$

又令 $v_p(0)=0$。两有理数 a,b 的 p 距离 $D_p(a,b)$ 的定义是

$$D_p(a,b)=v_p(a-b)。$$

定理1.18 p 赋值 v_p 有如下的性质：

1) $v_p(a)\geqslant 0$，$v_p(a)=0\Longleftrightarrow a=0$；

2) $v_p(ab)=v_p(a)v_p(b)$；

3) $v_p(a+b)\leqslant\max(v_p(a),v_p(b))$。

p 距离 D_p 有如下的性质：

1) $D_p(a,b)\geqslant 0$，$D_p(a,b)=0\Longleftrightarrow a=b$；

2) $D_p(a,b)=D_p(b,a)$；

3) 强三角不等式：$\max(D_p(a,b),D_p(b,c))\geqslant D_p(a,c)$。

因此 D_p 是一个距离(参考定义1.18)。

证明 很容易自 p 赋值 v_p 的定义 1.19，导出 1)，2)。现在看 v_p 的性质 3)。设

$$a=p^{l_1}\frac{m_1}{n_1},\qquad b=p^{l_2}\frac{m_2}{n_2},$$

又不妨假设 $l_1\leqslant l_2$。于是有

$$a+b=p^{l_1}\left(\frac{m_1}{n_1}+p^{l_2-l_1}\frac{m_2}{n_2}\right)=p^{l_1}\frac{m_1n_2+p^{l_2-l_1}n_1m_2}{n_1n_2}$$

$$=p^{l_1}\left(p^{l_3}\frac{m_3}{n_3}\right),\qquad l_3\geqslant 0。$$

即

$$v_p(a+b)=p^{-l_1-l_3}\leqslant p^{-l_1}=\max(p^{-l_1},p^{-l_2})$$
$$=\max(v_p(a),v_p(b))。$$

关于 p 距离 D_p 的三点性质。1)，2)皆很显然。性质 3)同等于 v_p 的性质 3)，即以

$$(a-b),\quad (b-c),\quad (a-c)=(a-b)+(b-c)$$

分别取代 v_p 的性质 3)中的 $a,b,a+b$，便得 D_p 的性质 3)。▌

讨论 1）在本书的后面关于"赋值"的讨论中读者将看出，Q 的任意赋值皆"同等"于绝对值或 p 赋值 v_p 之一。此种现象并不深奥，然而此时还不适宜于读者，所以暂时略去。

2）适合强三角不等式的距离 D，定义出一种奇异的几何学。例如任意三角形皆等腰，即取 a，b，c 为三角形的三顶点，如 $D(a,b)>D(b,c)>D(a,c)$，则

$$\max(D(a,c),D(c,b))<D(a,b)$$

为不可能。又例如圆内任意点皆是圆心，即如 a 是圆心，b 在圆内，c 在圆上，则有

$$D(a,c)=r>D(b,a),$$

$$\max(D(a,b),D(b,c))\geqslant D(a,c),$$

必有

$$D(b,c)=r.$$

定理1.19 令 $v_\infty(a)=|a|$，则有

$$v_\infty(a)\prod_p v_p(a)=1.$$

证明 显然。▎

定理1.20（赋值的独立性） 令 v_∞ 为绝对值。任取 v_∞ 及 n 个 p 赋值 $v_{p_1},v_{p_2},\cdots,v_{p_n}$。任取 $a,a_1,a_2,\cdots,a_n\in Q$，以及 $\varepsilon>0$，$p^{-l_1},p^{-l_2},\cdots,p^{-l_n}$，则存在 $b\in Q$，使

1）$v_\infty(b-a)=|b-a|<\varepsilon$；

2）$v_{p_i}(b-a_i)\leqslant p_i^{-l_i}$，$i=1,2,\cdots,n$。

证明 先用中国剩余定理来证明2）。令 m 为 $a_1,a_2,\cdots,a_n$ 的最小公分母。令

$$p_i^{-s_i}=v_{p_i}(m),\qquad r_i=l_i+s_i,$$

$$r=\max\{1,r_1,r_2,\cdots,r_n\}.$$

根据中国剩余定理，可得出一 c，使

$$c\equiv ma_i(\bmod p_i^{r_i}),\qquad i=1,2,\cdots,n.$$

即
$$v_{p_i}(c-ma_i)\leqslant p_i^{-t},\qquad v_{p_i}\left(\frac{c}{m}-a_i\right)\leqslant p_i^{-t}t.$$

令 $q=(p_1p_2\cdots p_n)^t$，取适当的整数 u，v，使
$$\left|\frac{c}{m}\ \frac{1+uq}{1+vq}-a\right|<\varepsilon.$$

令
$$b=\frac{c}{m}\ \frac{1+uq}{1+vq},$$

则 b 自然适合条件 1)。又由强三角不等式，有

$$\begin{aligned}v_{p_i}(b-a_i)&=v_{p_i}\left(\left(b-\frac{c}{m}\right)+\left(\frac{c}{m}-a_i\right)\right)\\&\leqslant\max\left(v_{p_i}\left(b-\frac{c}{m}\right),v_{p_i}\left(\frac{c}{m}-a_i\right)\right)\\&=v_{p_i}\left(\frac{c}{m}-a_i\right)\leqslant p_i^{-t}t.\quad\blacksquare\end{aligned}$$

以上的两个定理是讨论各赋值的关系。以下设 S 为一集合，D 为定义其上的一距离。根据本节的内容，可令 $S=\mathbf{Q}$，$D=D_\infty$ 或 D_p。然而，在本书后面的部分，我们将把同样的讨论，引用到一些广义的"环"上。为了避免重复论证起见，我们讨论一广义的集合 S。

定义1.20 取可数无限个 S 的直积 $\prod_{i=1}^{\infty}S$，其元素
$$\{a_i\}=(a_1,a_2,\cdots,a_n,\cdots)$$
称为**序列**。给定一个距离 D。如序列 $\{a_i\}$ 适合以下的条件，则称为**柯西序列**，或 **D 收敛序列**：对于任意有理数 $\varepsilon>0$，有一正整数 $N(=N(\varepsilon))$ 存在，使当 $m,n>N$ 时，
$$D(a_m,a_n)<\varepsilon.$$
所有柯西序列的集合，称为**柯西序列集** $F(D)$。

定义1.21 两柯西序列 $\{a_i\},\{b_i\}\in F(D)$，如适合以下的条件，则称**有共同的极限**，用符号

$$\{a_i\}\overset{D}{\sim}\{b_i\}$$

表示之：对任意的有理数 $\varepsilon>0$，有一正整数 $N(=N(\varepsilon))$存在，使当 $m>N$ 时，$D(a_m,b_m)<\varepsilon$。

定理1.21 柯西序列的有共同极限的关系是一等价关系（参考定义1.4的讨论）。

证明 1) $\{a_i\}\overset{D}{\sim}\{a_i\}$。显然。

2) $\{a_i\}\overset{D}{\sim}\{b_i\}$，则$\{b_i\}\overset{D}{\sim}\{a_i\}$。显然。

3) 设 $\{a_i\}\overset{D}{\sim}\{b_i\}\overset{D}{\sim}\{c_i\}$。给定 $\varepsilon>0$，则有一N存在，使当 $m>N$ 时，

$$D(a_m,b_m)<\frac{\varepsilon}{2},\qquad D(b_m,c_m)<\frac{\varepsilon}{2}.$$

用三角不等式，得出

$$D(a_m,c_m)\leqslant D(a_m,b_m)+D(b_m,c_m)<\varepsilon. \quad \blacksquare$$

定义1.22 由等价关系 $\overset{D}{\sim}$ 所产生的柯西序列集的商集(参考定义1.4及其后的讨论)称为S的D**完备化集**。每一个等价子集称为其元素的**极限**。如 $S=\mathbf{Q}$，D为由绝对值引生的距离 D_∞，则此完备化集称为**实数集 $\boldsymbol{R}$**。如 $S=\mathbf{Q}$，D为由 p 赋值 v_p 引生的距离 D_p，则此完备化集称 p-adic **数集 $\mathbf{Q}_p$**。

讨论 p-adic 数又称 p 进数。然而二进数、十进数等又是实数的一些表示法。如此，名词就混淆不清了。为此本书中用“p-adic 数”表示如上定义的 $\mathbf{Q}_p$，用 p 进数表示实数的 p 进位制。 $\blacksquare$

定义1.22给出了实数集 $\boldsymbol{R}$ 及 p-adic 数集 $\mathbf{Q}_p$ 的严格与完整的定义。以下我们要进一步地阐明其意义。

定理1.22 令D为S的一距离，S_D为相应的完备化集。则下列映射 φ: $S\to S_D$ 是一单射：

$$\varphi(a)=(a,a,\cdots,a,\cdots)=\{a\}.$$

证明 显然，$\{a\}$是一柯西序列。如 $a\neq b$，令 $\varepsilon=D(a,b)$，

则

$$D(a,b) \nless \varepsilon,$$

即$\{a\}$，$\{b\}$没有共同的极限。∎

如果我们把 Q 认同于 $\varphi(Q)$，则 Q 成了 Q_D 的子集。其次我们考虑怎样更具体地把 Q_D 写出来。如 $D=D_\infty$ 时，$Q_D=R$，我们有众所周知的十进位无穷小数表示法。这创始于中国商代，对于汉代的完美的数学工具是极重要的准备。根据以上的讨论，我们可以如下地理解这个十进位小数：任取一柯西序列$\{a_i\}$，取 $\varepsilon_j=10^{-j}$。令 N_j 为有如下性质的正整数(参考定义1.20)：如 $m,n>N_j$ 时，

$$D_\infty(a_m,a_n)=|a_m-a_n|\leqslant\varepsilon_j,$$

即 a_m 的十进位小数展开式与 a_{N_j+1} 的十进位小数展开式其小数点后$(j-1)$位全同。考虑 a_{N_j+1}，$j=1,2,3,\cdots,n,\cdots$，则小数逐渐确定了。取其极限，则得一无穷小数，即一般实数的无穷小数展开式。这种表示法并无唯一性。例如，$1=0.999\cdots9\cdots$。用柯西序列来说，即以下两个柯西序列

$$(1,1,1,\cdots,1,\cdots),$$

$$(0,0.9,0.99,\cdots,0.9999\cdots9,\cdots)$$

是有共同的极限的。

如同十进位无穷小数一样，我们可以同法得出 p-adic 数的 p 展开式：任取一分数 $a\in Q$，$a\neq0$。令

$$a=p^l\frac{m}{n},\quad p\nmid m,\ p\nmid n,\ l,m,n\in Z.$$

因为 p,n 互素，所以存在 $r,s\in Z$，使

$$sn+rp=1.$$

令 t 为$[sm]_p$ 的主余数，则有

$$[s(m-nt)]_p=[sm-snt]_p=[sm-t]_p=[0]_p,$$

于是有

$$p\,|\,m-nt,$$

$$a-tp^l=p^l\left(\frac{m}{n}-t\right)=p^l\frac{m-nt}{n}=p^{l+l'}\frac{m'}{n},$$

$$D_p(a,tp^l)\leqslant p^{-l-l'}<p^{-l}.$$

再以同法可以进一步展开 $p^{l+l'}\frac{m'}{n}$。如此逐步展开后，可得一p的幂级数，其系数皆取自$\{0,1,2,\cdots,p-1\}$。例如，令$p=3$，则$-1/6$的p-adic数的展开式是

$$-\frac{1}{6}=3^{-1}+1+3+3^2+3^3+\cdots+3^n+\cdots,$$

即

$$D_p\left(-\frac{1}{6},(3^{-1}+1+3+\cdots+3^n)\right)=3^{-(n+1)}\to 0.$$

不难看出，$\mathbf{Q}_p$即

$$\left\{\sum_{j=-n}^{\infty}c_jp^j:\ 0\leqslant j<p\right\}.$$

不同于十进位小数的是$\mathbf{Q}_p$的元素的p-adic数的展开式是唯一的。

定义1.23 在$\boldsymbol{R}$中定义不等式如下：取$\alpha,\beta\in\boldsymbol{R}$，令$\{a_i\}$，$\{b_i\}$为以$\alpha,\beta$为极限的两柯西序列。任取$\varepsilon>0$，如有$N$存在，使$i>N$时，有

$$a_i\geqslant b_i-\varepsilon,$$

则称$\{a_i\}\geqslant\{b_i\}$及$\alpha\geqslant\beta$。如$\alpha\geqslant\beta$且$\alpha\neq\beta$，则称$\alpha>\beta$。

定理1.23 以上定义的不等式有如下的性质：

1）如柯西序列$\{a_i\},\{a'_i\}$有共同的极限，$\{b_i\},\{b'_i\}$有共同的极限，则

$$\{a_i\}\geqslant\{b_i\}\iff\{a'_i\}\geqslant\{b'_i\}.$$

此即不等式在$\boldsymbol{R}$中是有意义的；

2）如$\alpha\geqslant\beta$，$\beta\geqslant\alpha$，则$\alpha=\beta$；

3）如$\alpha\geqslant\beta\geqslant\gamma$，则$\alpha\geqslant\gamma$；

4) 任取 $\alpha,\beta\in\boldsymbol{R}$，必有 $\alpha\geq\beta$ 或 $\beta\geq\alpha$。

证明 读者试自证之。▎

我们把四则运算自 $\boldsymbol{Q}$ 扩充到 $\boldsymbol{Q}_D$。请注意如一柯西序列$\{a_i\}$不以 0 为极限，则其仅有有限多个 a_i 可为 0。即 $\boldsymbol{Q}_D$ 的任意元素 α，如不为零，皆有一柯西序列$\{a_i\}(a_i\neq0)$以 α 为极限。

定义1.24 任取$\alpha,\beta\in\boldsymbol{Q}_D$。令$\{a_i\}$是以 α 为极限的柯西序列，$\{b_i\}$是以 β 为极限的柯西序列，则$\{a_i+b_i\},\{a_i-b_i\},\{a_ib_i\}$皆是柯西序列，其极限分别定义为$\alpha+\beta,\alpha-\beta,\alpha\beta$。如$\alpha\neq0$，设$\{a_i\}$以 α 为极限，并且 $a_i\neq0$，则$\{b_i/a_i\}$是一柯西序列，其极限定义为 β/α。

讨论 读者试自证，以上的定义与$\{a_i\},\{b_i\}$无关，仅与其极限有关。即，如$\{a_i\}\overset{D}{\sim}\{a'_i\}$，$\{b_i\}\overset{D}{\sim}\{b'_i\}$，则有

$$\{a_i+b_i\}\overset{D}{\sim}\{a'_i+b'_i\}$$

等等。▎

以下，我们把距离D，自 S 扩充到 S_D，并且还用同一符号D表示之。

定义1.25 任取两柯西序列$\{a_i\},\{b_i\}$，我们定义 $D(\{a_i\},\{b_i\})$为一序列$\{c_i\}$，这里

$$c_i=D(a_i,b_i).$$

在下一定理中，我们在 S_D 中取距离D，在 $\boldsymbol{R}$ 中取距离 D_∞

定理1.24 1) $D(\{a_i\},\{b_i\})$是 D_∞ 柯西序列；

2) 如$\{a_i\}$与$\{a'_i\}$有共同的极限 α，$\{b_i\}$与$\{b'_i\}$有共同的极限 β，则 $D(\{a_i\},\{b_i\})$与$D(\{a'_i\},\{b'_i\})$有共同的极限，记为$D(\alpha,\beta)$；

3) D 是 S_D 的一距离。

证明 1) 任取 $\varepsilon>0$，则有 $N(a),N(b)$，使

$$D(a_m,a_n)<\varepsilon/2,\qquad 当\ m,n>N(a),$$
$$D(b_m,b_n)<\varepsilon/2,\qquad 当\ m,n>N(b).$$

取 $N=\max(N(a),N(b))$。于是当 $m,n>N$ 时，利用三角不等

式——在下式中假设$D(a_m,b_m)\geqslant D(a_n,b_n)$——有

$$D_\infty(c_m,c_n)=|c_m-c_n|=|D(a_m,b_m)-D(a_n,b_n)|$$
$$\leqslant|D(a_m,a_n)+D(a_n,b_n)+D(b_n,b_m)-D(a_n,b_n)|$$
$$=|D(a_m,a_n)+D(b_m,b_n)|<\varepsilon,$$

即$D(\{a_i\},\{b_i\})$是D_∞柯西序列。

2) 令$D(\{a'_i\},\{b'_i\})=\{c'_i\}$。任取$\varepsilon>0$,则有$N(a)$及$N(b)$,使

$$D(a_n,a'_n)<\varepsilon/2,\qquad 当\ n>N(a),$$
$$D(b_n,b'_n)<\varepsilon/2,\qquad 当\ n>N(b).$$

取$N=\max(N(a),N(b))$,于是当$n>N$时——假设$c_n>c'_n$——有

$$D_\infty(c_n,c'_n)=|c_n-c'_n|=|D(a_n,b_n)-D(a'_n,b'_n)|$$
$$\leqslant|D(a_n,a'_n)+D(a'_n,b'_n)+D(b'_n,b_n)-D(a'_n,b'_n)|$$
$$=|D(a_n,a'_n)+D(b_n,b'_n)|<\varepsilon.$$

3) 根据 1)及 2),D是定义在S_D上的非负实值二元函数。现要证明D是一距离。很容易验证距离的三项性质的前两项。我们仅证明第三项,即三角不等式。令$\alpha,\beta,\gamma\in S_D$,$\{a_i\},\{b_i\}$,$\{c_i\}$为三柯西序列,分别以$\alpha,\beta,\gamma$为极限。任取$\varepsilon>0$,则有一共同的$N$存在,使$m>N$时,有

$$D(a_m,b_m)\geqslant D(a_N,b_N)-\frac{\varepsilon}{3},\quad D(b_m,c_m)\geqslant D(b_N,c_N)-\frac{\varepsilon}{3},$$

$$D(a_N,c_N)\geqslant D(a_m,c_m)-\frac{\varepsilon}{3}.$$

于是有

$$D(a_m,b_m)+D(b_m,c_m)>D(a_N,b_N)+D(b_N,c_N)-\frac{2\varepsilon}{3}$$

$$\geqslant D(a_N,c_N)-\frac{2\varepsilon}{3}\geqslant D(a_m,c_m)-\varepsilon.$$

根据定义1.24及1.23,得

$$\{D(a_i,b_i)\}+\{D(b_i,c_i)\}=\{D(a_i,b_i)+D(b_i,c_i)\}$$
$$\geqslant\{D(a_i,c_i)\},$$

即
$$D(\alpha,\beta)+D(\beta,\gamma)\geqslant D(\alpha,\gamma). \blacksquare$$

我们要证明，S对距离D的完备化集S_D是"完备的"，我们给出以下的定义。

定义1.26 设D为集合S的一距离，如适合下列的条件，则称S对D是完备的：S的任一柯西序列$\{a_i\}$，皆有一极限点。即，如$\{a_i\}$为D柯西序列，则存在$a\in S$，使对任意的$\varepsilon>0$，有一正整数$N=N(\varepsilon)$，只要$n>N$，则有

$$D(a_n,a)<\varepsilon.$$

定理1.25 设S为一集合，D为S的一距离，则S的D完备化集S_D是完备的。

证明 令$\{\alpha_i\}$为S_D的一D柯西序列。对每个$\alpha_i\in S_D$，取S中的一柯西序列$\{a_{ij}\}=(a_{i1},a_{i2},\cdots,a_{in},\cdots)$，使其以$\alpha_i$为极限。令$N(i)$为有下列性质的正整数：当$m,n\geqslant N(i)$时，

$$D(a_{im},a_{in})<\frac{1}{i}.$$

适当地加大$N(i)$以后，不妨设
$$N(1)<N(2)<\cdots<N(i)<N(i+1)<\cdots.$$
令$b_i=a_{i,N(i)}$。将证：1）$\{b_i\}$是D柯西序列（于是令α为$\{b_i\}$的极限，α自然在S_D中）；2）α是$\{\alpha_i\}$的极限点（如此则知S_D是完备的）。

先证1)。给定一$\varepsilon>0$。因$\{\alpha_i\}$是S_D的D柯西序列，故存在一N_1，当$m,n>N_1$时，有

$$\{D(a_{ml},a_{nl})\}<\left\{\frac{\varepsilon}{6}\right\}=\left(\frac{\varepsilon}{6},\frac{\varepsilon}{6},\cdots,\frac{\varepsilon}{6},\cdots\right).$$

参考定义1.23，知存在一正整数$N_2(m,n)$，使$l>N_2(m,n)$时，

有

$$D(a_{ml},a_{nl})<\frac{\varepsilon}{3}.$$

取 N_3，使$\frac{1}{N_3}<\frac{\varepsilon}{3}$. 令 $N=\max(N_1,N_3)$. 任取 $m,n>N$，利用三角不等式，则有

$$\begin{aligned}D(b_m,b_n)&=D(a_{m,N(m)},a_{n,N(n)})\\&\leqslant D(a_{m,N(m)},a_{ml})+D(a_{ml},a_{nl})\\&\quad+D(a_{nl},a_{n,N(n)})\\&<\frac{\varepsilon}{3}+\frac{\varepsilon}{3}+\frac{\varepsilon}{3}=\varepsilon.\end{aligned}$$

此处 $l>\max(N_2(m,n),N(m),N(n))$. 于是$\{b_l\}$是$D$柯西序列.

2) 利用 1)中已证出的结果. 任取 ε_1，令 $\varepsilon=\varepsilon_1/2$. 按照 1)的证法，得一正整数$N$. 设 $l,n>N$，令

$$s>\max(N_2(n,l),N(n),N(l)),$$

利用三角不等式，有

$$\begin{aligned}D(a_{nl},b_l)&=D(a_{nl},a_{l,N(l)})\\&\leqslant D(a_{nl},a_{ns})+D(a_{ns},a_{ls})\\&\quad+D(a_{ls},a_{l,N(l)})\\&<\frac{\varepsilon}{3}+\frac{\varepsilon}{3}+\frac{\varepsilon}{3}=\varepsilon.\end{aligned}$$

按照定义1.23，得$\{D(a_{nl},b_l)\}\leqslant\varepsilon$，即

$$D(a_n,a)\leqslant\varepsilon<\varepsilon_1. \quad \blacksquare$$

习　题

1. 设 $\mathbf{Q}_{11}$ 内两个数 α,β:

$$\alpha=3+7\times11+9\times11^2+2\times11^3+7\times11^4+\cdots,$$

$$\beta=8+2\times11+5\times11^2+10\times11^3+11^4+\cdots,$$

试计算 $\alpha+\beta$ 的表达式到第五个数位.

2. 设 $a\in\mathbf{Q}$，它在 $\mathbf{Q}_p$ 内的表达式为

$$a=a_{-m}p^{-m}+a_{-m+1}p^{-m+1}+\cdots+a_0+a_1p+\cdots,$$

试求 $-a$ 的表达式。

3. 在 $\mathbf{Q}_7$ 内计算：

$$(6+4\times7+2\times7^2+1\times7^3+\cdots)(3+0\times7+0\times7^2+6\times7^3+\cdots)$$

到第四个数位。

4. 在 $\mathbf{Q}_5$ 内求 a，使

$$a(3+2\times5+3\times5^2+1\times5^3+\cdots)=1,$$

计算到第四个数位。

5. 设 $a\in\mathbf{Q}_p$，如果它的 p-adic 表达式中只有有限多个系数不为零，证明 a 是正有理数，且其分母为 p 的方幂。

6. 证明在 $\mathbf{Q}_5$ 内 6 可以开平方，即存在

$$(a_0+a_1\times5+a_2\times5^2+\cdots)^2=1+1\times5\quad(0\leqslant a_i\leqslant4).$$

7. 证明在 $\mathbf{Q}_5$ 内 7 不能开平方。

8. 设 $a\in\mathbf{Q}_p$。证明 a 的 p-adic 表达式

$$a=a_{-m}p^{-m}+a_{-m+1}p^{-m+1}+\cdots+a_0+a_1p+\cdots$$

从某处起数位循环(即对某个正整数 r 和某个整数 N，当 $i>N$ 时有 $a_{i+r}=a_i$)当且仅当 $a\in\mathbf{Q}$。

9. 给定 $\mathbf{Q}_p$ 内一个级数

$$a_1+a_2+a_3+\cdots.$$

如果它的部分和序列

$$S_n=a_1+a_2+\cdots+a_n$$

有极限，则称该级数收敛。证明级数 $\sum a_n$ 收敛的充要条件是

$$\{a_n\}=\{0\}.$$

10. 证明在 $\mathbf{Q}_p$ 内方程 $x^p-x=0$ 有 p 个解。

11. 证明$\left\{1+\frac{1}{2!}+\cdots+\frac{1}{n!}:n=1,2,3,\cdots\right\}$对任何 p-adic 赋值而言，不是一个柯西序列，因此，在 $\mathbf{Q}_p$ 内 e 没有定义。

12. 证明：如 $p|x(x\in\mathbf{Z})$，那么，对 p-adic 赋值而言，序列

$$\left\{1+x+\frac{x^2}{2!}+\cdots+\frac{x^n}{n!}\right\}$$

是一个柯西序列，于是在 Q_p 内 e^x 有意义。

13. 已知有广义二项式定理如下：

$$(1+x)^l=1+\sum_{i=1}^{+\infty}\binom{l}{i}x^i,$$

其中 $l\in Q$，而

$$\binom{l}{i}=\frac{l(l-1)\cdots(l-i+1)}{i!}.$$

试证明在 Q_3 内有

$$\frac{5}{2}=3-\frac{1}{1-3}=1+2\times3+3^2+\cdots+3^n+\cdots.$$

于是有：

$$\begin{aligned}(1+x)^{5/2}&\equiv(1+x)(1+x)^{2\times3}(1+x)^{3^2}\cdots\\&\equiv(1+x)(1+x^3)^2(1+x^{3^2})\cdots(1+x^{3^n})\cdots(\bmod 3).\end{aligned}$$

第二章 群 论

§1 群的定义

定义2.1 设G为一非空集合．如果任取G中的二元素a及b，$a*b$也是G中的一个元素，则称“$*$”为一个**双项运算**．如果对G的一个子集H而言，从H中任意两个元素a及b得到的$a*b$恒在H中，则称H对$*$是**封闭的**，即$*$为H的双项运算．

在整数集合中，加、减、乘都是双项运算，而除法则不是双项运算，因为除法运算的结果可能是一非整数，甚至为无穷大．

定义2.2 设G为一非空集合，$*$为一双项运算，如有下列性质，则称$(G,*)$(简言之，G)为一**群**．

1）**结合律**．即对任意的$a,b,c\in G$，恒有

$$(a*b)*c=a*(b*c).$$

2）**幺元**．即存在一元素$e\in G$，使得G中任意元素a皆适合

$$e*a=a*e=e.$$

3）**逆元素**．G中任意元素a皆有对$*$的逆元素，即有一元素$b\in G$，适合

$$a*b=b*a=e.$$

讨论 1）结合律的意义是双项运算$*$的结果与运算顺序的先后无关，所以我们可以定义

$$a*b*c=a*(b*c)=(a*b)*c.$$

在一般运算中可以省去括号．

2）幺元的唯一性．设另有一幺元e'，则有

$$e=e*e'=e'.$$

故得幺元的唯一性．

3）逆元素的唯一性．设b及b'皆为一元素a的逆元素，则有

$$b=b*(a*b')=(b*a)*b'=b'.$$

故得逆元素的唯一性。一元素 a 的逆元素通常以 a^{-1} 表示之。

4) 通常以 a^n 表示 $a*a*\cdots*a$，式中有 n 个 a。通常以 a^{-n} 表示 $a^{-1}*a^{-1}*\cdots*a^{-1}$，式中有 n 个 a^{-1}。

5) 使得 $a^n=e$ 的最小的正整数 n，称为元素 a 的阶，记为 $o(a)=n$。如果 a^n 永不等于 e，则称 a 的阶为无穷大，记为 $o(a)=\infty$。

6) 易见 a_1*a_2 的逆元素是 $a_2^{-1}*a_1^{-1}$。同理，$a_1*a_2*\cdots*a_n$ 的逆元素是 $a_n^{-1}*\cdots*a_2^{-1}*a_1^{-1}$。 ▍

群的定义至为简单，因此群的范围涵盖很广。我们可以把群的概念引入许多集合之中，例如数字的集合、物体对换的集合、空间的运动集合、向量空间的线性变换集合等，从而得出这些集合内的群论的数学关系。现在我们要研究一些例子。

例 1 整数集合 $\boldsymbol{Z}$ 对加法"+"而言是一群。$\boldsymbol{Z}$ 对乘法"·"而言并非一群。这因为它不适合定义中的"逆元素"的条件，例如 2 并无整数为其逆元素。

$(\{0\},+)$ 及 $(\{1\},\cdot)$ 皆为群。这类由双项运算的幺元所构成的群，称之为**幺群**。

$\{\boldsymbol{Z}_n,+\}$ 是一群，这个群是由 $[1]_n$ 累次相加所生成的。类似地，整数加群 $\{\boldsymbol{Z},+\}$ 是由 1 及其逆元素 -1 累次相加所生成的。一般言之，如果一群 G 是由某一元素 a 及其逆元素 a^{-1} 累次进行双项运算所生成的，则称 G 为一**循环群**。

例 2 n 个物体的**对称群** S_n。不妨设这 n 个物体为整数 1，2，…，n。S_n 是 $\{1,2,\cdots,n\}$ 到自身的单满映射的集合，此群中两个元素的双项运算定义为映射的**合成**，即

$$(\sigma*\delta)(i)=\sigma(\delta(i)),\quad i=1,2,\cdots,n.$$

此群中的元素 σ 可以表成

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{pmatrix},$$

式中的下行为 $(1,2,\cdots,n)$ 的另一排列。此种排列的个数为

$n!$，故知 S_n 的基数是 $n!$。

例3 平面上的平移群、反射群、旋转群及刚体运动群。令 $\{O;X,Y\}$ 为平面上的一直角坐标系，(x,y) 为任意点的坐标。此四群中的元素都是平面上的单满映射，而其双项运算都是映射的合成。

平移群由平移 $\beta_{ab}(a,b\in \mathbf{R})$ 组成，β_{ab} 对平面的作用定义如下：

$$\beta_{ab}(x,y)=(x+a,y+b)。$$

不难看出

$$\beta_{ab}*\beta_{cd}=\beta_{a+c,b+d}。$$

由此可得：β_{00} 是幺元，而 β_{ab} 的逆元素是 $\beta_{-a,-b}$。

取平面上的一直线 l，对此直线的全体镜象映射构成一群，这就是**反射群**。为简便起见，不妨假定这条直线即是Y轴，则镜象映射如图2.1所示。镜象映射 γ 的作用如下：

$$\gamma(x,y)=(-x,y)。$$

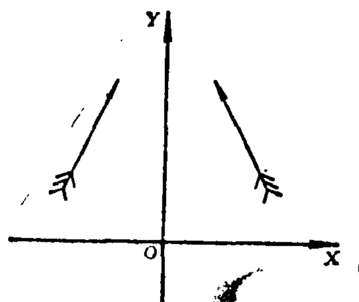


图 2.1

不难看出 $\gamma*\gamma=e$（e 表示幺映射，即 $e(x,y)=(x,y)$）。反射群中只有两个元素 e 及 γ。

平面上以一点为旋转心的所有旋转构成一群，即所谓**旋转群**。为简便起见，不妨假定此旋转心即原点。令旋转角为 $\theta(0\leqslant\theta<360°)$ 的旋转为 ρ_θ。不难看出

$$\rho_{\theta_1}*\rho_{\theta_2}=\rho_{[\theta_1+\theta_2]},$$

其中$[\theta_1+\theta_2]$表示$\theta_1+\theta_2$对模360°的正余数。在此群中ρ_0为幺元，ρ_θ的逆元素是$\rho_{[-\theta]}$。

保持平面上的所有点之间的距离的平面到自身的映射所构成的群，称之为**刚体运动群**。不难看出，此种刚体运动必然把直线映射成直线，并且保持两直线的交角不变，其理由可见图2.2。

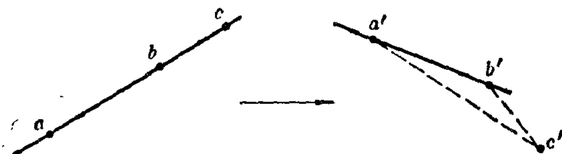


图 2.2

如a,b及b,c的距离分别等于a',b'及b',c'的距离，而c'不在过a'，b'的直线上，则a',c'的距离必小于a，c的距离，这与刚体运动的定义不符。同理，只要连接两条相交的直线，成一三角形，便可看出两直线的交角在刚体运动下不变。

取一刚体运动m。设m把原点$(0,0)$映成(a,b)点，则有

$$(\beta_{-a,-b}*m)(0,0)=\beta_{-a,-b}(a,b)=(0,0),$$

即$\beta_{-a,-b}*m$不移动原点。取一适当的旋转角θ，以旋转平面使Y轴重合，即

$$\rho_\theta*\beta_{-a,-b}*m(0,y)=(0,y).$$

此时X轴或重合，或恰好反方向，也即

$$\rho_\theta*\beta_{-a,-b}*m=e \quad 或 \quad \gamma*\rho_\theta*\beta_{-a,-b}*m=e.$$

由此可得

$$m=\beta_{ab}*\rho_{[-\theta]} \quad 或 \quad m=\beta_{ab}*\rho_{[-\theta]}*\gamma.$$

即任意刚体运动皆是由平移、旋转及反射生成的。

例4 在物理学中有**伽利略群**及**罗伦兹群**。为简明起见，设空间为一维，以X轴表示之；时间为另一维，以T轴表示之。设另一坐标系$\{X',T\}$以速度u平稳地向X轴的右方运动。则伽利略群的元素g_u可表成如下的映射：

$$g_u\begin{pmatrix} x \\ t \end{pmatrix} = \begin{pmatrix} x' \\ t \end{pmatrix} = \begin{pmatrix} x-ut \\ t \end{pmatrix}.$$

不难看出

$$g_u * g_v = g_u \circ g_v = g_{u+v},$$

而且时间轴不受运动的影响。伽利略群与牛顿力学有密切的关系。在牛顿力学中，时间是不受运动影响的。

罗伦兹群的元素$\mathscr{L}_u$的定义如下

$$\mathscr{L}_u\begin{pmatrix} x \\ t \end{pmatrix} = \begin{bmatrix} \dfrac{x-ut}{\sqrt{1-u^2/c^2}} \\ \dfrac{t-ux/c^2}{\sqrt{1-u^2/c^2}} \end{bmatrix} = \begin{pmatrix} x' \\ t' \end{pmatrix},$$

其中c是光速。经简单计算，我们得出

$$\mathscr{L}_u * \mathscr{L}_v = \mathscr{L}_u \circ \mathscr{L}_v = \mathscr{L}_w,$$

此处w满足

$$\frac{w}{c} = \frac{(u/c)+(v/c)}{1+uv/c^2}.$$

不难证明，如果$|u|<c$，$|v|<c$，则有$|w|<c$，即罗伦兹群中所有适合$|u|<c$的元素$\mathscr{L}_u$自成一较小的群。这是物理中极有趣味的现象：我们可以设想一太空飞船以速度v离开地球，而此飞船又发射一相对于它的速度为u的火箭。则从地球上观测，此火箭的速度为w而不是$u+v$。如果u,v皆小于c，则w也小于c。此即物理学中"光速不可超过"的定律。此定律其实不外乎罗伦兹群内某种群论的关系。罗伦兹群与电磁学有密切的关系，更是特殊相对论的基石。

例 5　线性群$\mathrm{GL}(n,\boldsymbol{R})$。取行列式不为零的$n\times n$实数矩阵，构成一个集合。在此集合中取矩阵的乘法为双项运算，则此集合成为一群。其理由如下：以 $\det A$ 表示矩阵 A 的行列式，线性代数中有如下的公式：

$$\det(AB) = \det A \det B,$$

故知$\mathrm{GL}(n,\boldsymbol{R})$对乘法而言是封闭的；在线性代数中又有

$$A(BC) = (AB)C,$$

故知乘法有结合律；又知幺矩阵 I_n 的行列式为1，而且

$$I_nA = AI_n = A,$$

故 I_n 即乘法的幺元。又由线性代数知行列式不为零的矩阵 A 皆有逆矩阵 A^{-1}，A^{-1}的行列式显然不为零，故在 $\mathrm{GL}(n,\boldsymbol{R})$中。所以 $\mathrm{GL}(n,\boldsymbol{R})$对矩阵乘法构成一群。

此群可以理解为 n 维向量空间 $\boldsymbol{R}^n$ 上的非奇异的线性变换所构成的群。

习　题

1. 若集合G非空，G中有双项运算"$*$"，$*$满足结合律，则称G(对运算$*$)构成半群(semigroup)。若G为半群，且存在$e\in G$，使得$a*e=e*a=a(\forall a\in G)$，则称$G$为幺半群(monoid)。

(1) 证明偶数集合$2\boldsymbol{Z}$对通常乘法构成半群，但不是幺半群；

(2) 在$2\boldsymbol{Z}$中定义运算$*$：

$$a*b=a+b+ab \quad (\forall a,b\in 2\boldsymbol{Z}),$$

证明$2\boldsymbol{Z}$对运算$*$构成幺半群。

2. 证明群的定义可改述如下：设G为非空集合，$*$为G中的双项运算。如果：(1) $*$有结合律；(2) G中存在左幺元e'，即对任意的$a\in G$，总有$e'a=a$；(3) G中任一元素a有左逆元a'，即$a'a=e'$，则称G为群。

证明在上述定义中的"左"都改成"右"也是可以的。

试举一例，说明将上述定义中的(1)，(2)保留，将(3)改成"G中任一元素有右逆元"，G可以不是群。

3. 证明群的定义可改述为：设G为非空集合，$*$为G中双项运算，如果：(1) $*$有结合律；(2) 对任意的$a,b\in G$，方程$ax=b$及$ya=b$都恒有解，则称G为群。

4. 在一个有双项运算$*$的集合S中，如果

$$a*b=a*c \Longrightarrow b=c \quad (\forall a,b,c\in S),$$

则称S有左消去律。同样，

$$b * a = c * a \Longrightarrow b = c \quad (\forall a, b, c \in S),$$

则称 S 有**右消去律**。证明运算适合结合律且有左、右消去律的非空有限集合是群。

5. 以 $\mathrm{FL}(n, \boldsymbol{R})$ 表示所有 $n \times n$ 的实数矩阵的集合。证明对通常的加法而言，$\mathrm{FL}(n, \boldsymbol{R})$ 是一个群，称为**全线性群** (full linear group)。

6. 令 $\mathrm{SL}(n, \boldsymbol{R}) = \{A: A \in F(n, \boldsymbol{R}), \det A = 1\}$，证明 $\mathrm{SL}(n, \boldsymbol{R})$ 对乘法成群，称为**特殊线性群**(special linear group)。

7. **四元数集** (quaternion)是指集合 $\{(a_0, a_1, a_2, a_3): a_i \in \boldsymbol{R} (\forall i = 0, 1, 2, 3)\}$。通常写成

$$(a_0, a_1, a_2, a_3) = a_0 + a_1 i + a_2 j + a_3 k,$$

i, j, k 适合下列乘法规律：

$$1 \cdot i = i, \quad 1 \cdot j = j, \quad 1 \cdot k = k,$$

$$i^2 = j^2 = k^2 = -1,$$

$$k = i \cdot j = -j \cdot i, \quad i = j \cdot k = -k \cdot j, \quad j = k \cdot i = -i \cdot k.$$

一般元素乘法按分配律进行。证明非零四元数集关于乘法构成群。

8. 设 I 为一个指标集合。任取一些群 $G_i (i \in I)$，令 e_i 是 G_i 的幺元。定义

$$\bigoplus_{i \in I} G_i = \{(\cdots, a_i, \cdots): a_i \in G_i, \text{除有限多个 } i \text{ 以外，} a_i = e_i\},$$

称之为 $\{G_i: i \in I\}$ 的**直和**(direct sum)。定义

$$(\cdots, a_i, \cdots)(\cdots, b_i, \cdots) = (\cdots, a_i b_i, \cdots).$$

证明 $\bigoplus_{i \in I} G_i$ 是一个群。

9. G_i 如题8。定义

$$\prod_{i \in I} G_i = \{(\cdots, a_i, \cdots): a_i \in G_i\},$$

称之为 $\{G_i: i \in I\}$ 的**直积**(direct product)。定义

$$(\cdots, a_i, \cdots)(\cdots, b_i, \cdots) = (\cdots, a_i b_i, \cdots).$$

证明 $\prod_{i \in I} G_i$ 是一个群。

10. 以 I_n 表示 GL(n,$\boldsymbol{R}$)的幺元。令

$$J=\begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix}\subset \mathrm{GL}(2n,\boldsymbol{R}),$$

A^T 表示A的转置(transpose)。定义

$$\mathrm{Sp}(2n,\boldsymbol{R})=\{A:\ A\in \mathrm{GL}(2n,\boldsymbol{R}),\ A^TJA=J\}.$$

证明：Sp($2n$,$\boldsymbol{R}$) 对矩阵乘法构成群，称之为**辛群** (symplectic group)。

11. 设群G有n个元素$a_1,a_2,\cdots,a_n$。矩阵

$$\begin{bmatrix} a_1a_1 & a_1a_2 & \cdots & a_1a_n \\ a_2a_1 & a_2a_2 & \cdots & a_2a_n \\ \cdots & \cdots & \cdots & \cdots \\ a_na_1 & a_na_2 & \cdots & a_na_n \end{bmatrix}$$

被称为G的**乘法表**。

(1) 写出$\boldsymbol{Z}_3$对加法构成的群和$\boldsymbol{Z}_{12}^*$对乘法构成的群的乘法表；

(2) 证明乘法表的每一行(列)的元素都不相同。

我们可以有如下的应用：我们进行农业实验，用n种不同的肥料及n种不同的农药(设已知肥料与农药不相干扰)和n种不同的作物.我们把方形实验田分割成n行及n列，在每一行中施用不同的肥料，每一列中施用不同的农药。试用G的乘法表安排n种作物，使每一种作物都试遍了各种肥料和农药。

12. 证明：任给平面上的刚体运动σ，都可以写成一些反射$\gamma_1,\gamma_2,\cdots,\gamma_n$的乘积，即$\sigma=\gamma_1\gamma_2\cdots\gamma_n$。所以平面上的刚体运动群是由反射生成的。

13. 同样地，证明三度空间中的刚体运动群是由反射生成的。

§2 集合上的变换群

定义2.3 取一群G及一集合S。如果G中任意元素g皆为S的映射，且G的任意二元素g_1,g_2，G的幺元e及S的任意元素s，

皆适合下列公式：

1） $(g_1 * g_2)(s) = g_1(g_2(s))$，

2） $e(s) = s$，

则称 G 为 S 的变换群。

讨论 不仅第一节中的例2，例5皆是集合上的变换群，而且任意群 $(G, *)$ 都可理解为集合 G 的变换群。事实上，对 G 中的任一元素 g，规定集合 G 的一个映射如下：

$$g(a) = g * a,$$

此处 a 为集合 G 的任意元素。不难看出，在此规定下，群 G 是集合 G 的一个变换群。

定理2.1 如果 G 为 S 的变换群，则 G 中的任意元素 g 皆为 S 的单满映射。

证明 1） g 为单射。如有 $g(s_1) = g(s_2)$，则

$$g^{-1}(g(s_1)) = g^{-1}(g(s_2)).$$

即有

$$(g^{-1} * g)(s_1) = (g^{-1} * g)(s_2), \quad e(s_1) = e(s_2), \quad s_1 = s_2.$$

2） g 为满射。设 s 为 S 的任意元素，令 $s' = g^{-1}(s)$，则

$$g(s') = g(g^{-1}(s)) = (g * g^{-1})(s) = e(s) = s. \quad \blacksquare$$

研究集合 S 的变换群 G，其着眼点是 G 对 S 的作用，及在此作用下 S 与 G 的相互影响。我们引入如下的定义：

定义2.4 设 G 为集合 S 的变换群。S 的一个元素 s 的轨道 $\mathrm{Orb}(s)$ 定义为 $\mathrm{Orb}(s) = \{g(s): g \in G\}$。

例6 参考上一节，考虑平移群、反射群及旋转群的轨道。

不难看出，在平移群的作用下，平面上任一点的轨道都是整个平面。

在反射群作用下，平面上的任一点与其镜象点构成一轨道。如此点不在反射轴（在上节讨论中，轴 l 即 Y 轴）上，则其轨道由两点组成；反之，则仅由此点本身构成。

在旋转群作用下，平面上任一点的轨道是通过此点、以旋转

心为圆心的圆。如此点是旋转心，则其轨道仅有一点。

例7 平面上的任意二次曲线，皆是某群作用下的轨道。

任意取一抛物线，经过坐标变换简化其方程式后，不妨假定此抛物线是由下式定义的：

$$y = x^2.$$

取一群$G_1 = \{\tau_a: a \in \boldsymbol{R}\}$，其双项运算$*$定义如下：

$$\tau_a * \tau_b = \tau_{a+b}.$$

群G_1对平面的作用定义为

$$\tau_a(x, y) = (x + a, y + 2ax + a^2).$$

不难看出，幺元τ_0以及二元素τ_a, τ_b适合以下关系：

$$\tau_0(x, y) = (x, y),$$

$$\begin{aligned}\tau_b(\tau_a(x, y)) &= \tau_b(x + a, y + 2ax + a^2)\\ &= (x + a + b, y + 2(a + b)x + (a + b)^2)\\ &= \tau_{a+b}(x, y) = (\tau_a * \tau_b)(x, y).\end{aligned}$$

故G_1为平面上的变换群，而且

$$\mathrm{Orb}((0,0)) = \{(a, a^2): a \in \boldsymbol{R}\} = \{(x, y): y = x^2\}.$$

即$\mathrm{Orb}((0,0))$就是我们开始所说的那条抛物线。

不难看出，$\mathrm{Orb}((c,d))$是如下方程式所定义的抛物线：

$$y^2 = x^2 - (c^2 - d).$$

这类抛物线或完全重合，或不相交。

双曲线的情形也类似。不妨假定此双曲线是由下式定义的：

$$xy = 1.$$

令$G_2 = \{\sigma_a: a \neq 0,\ a \in \boldsymbol{R}\}$，其双项运算$*$定义如下：

$$\sigma_a * \sigma_b = \sigma_{ab}.$$

群G_2对平面的作用定义为

$$\sigma_a(x, y) = (ax, a^{-1}y).$$

不难看出，$\mathrm{Orb}((1,1))$即是上述的双曲线。其余各轨道分别为

$$\mathrm{Orb}((0,0)) = \{(0,0)\};$$

$$\mathrm{Orb}((c,0)) = X\text{轴}\setminus\{(0,0)\};$$

$$\mathrm{Orb}((0,d)) = Y\text{轴}\setminus\{(0,0)\};$$

而$\mathrm{Orb}((c,d))$为由下式定义的双曲线：

$$xy = cd.$$

（以上c,d皆为非零实数．）这些轨道或完全重合，或不相交．

再考虑任一椭圆．经过坐标变换以后，不妨假定其方程式为

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1,$$

其中$a \geq b > 0$．令$G_3 = \{\delta_\theta : 0 \leq \theta < 360°\}$，其双项运算$*$定义如下：

$$\delta_{\theta_1} * \delta_{\theta_2} = \delta_{[\theta_1 + \theta_2]},$$

其中$[\theta_1 + \theta_2]$是$\theta_1 + \theta_2$对模360°的主余数．G_3对平面的作用定义为

$$\delta_\theta(x,y) = (ar\cos\theta, br\sin\theta),$$

其中

$$r = \sqrt{\frac{x^2}{a^2} + \frac{y^2}{b^2}}.$$

不难看出，上述的椭圆即$\mathrm{Orb}((a,0))$．其余的轨道或是由原点构成，或是由下列方程式所定义的椭圆：

$$\frac{x^2}{(ac)^2} + \frac{y^2}{(bc)^2} = 1,$$

其中$c \in \boldsymbol{R}, c \neq 0, 1$．这些轨道或完全重合，或不相交．▌

从上面的例子可以发现一规律性：这些轨道或完全重合，或不相交．这种“分离性”是轨道共有的性质．我们可以证明如下的定理．

定理2.2 设G是S的变换群，则S是各轨道的并集，而各轨道均是分离的．

证明 1) S是轨道的并集．令s为S的任一元素．则

$$e(s) = s.$$

故$s \in \mathrm{Orb}(s)$．

2) 轨道是分离的．设

$$\mathrm{Orb}(s_1) \cap \mathrm{Orb}(s_2) \neq \varnothing.$$

取$s_3 \in \mathrm{Orb}(s_1) \cap \mathrm{Orb}(s_2)$，则有$s_3 = g_1(s_1) = g_2(s_2)$．故

$$s_1=g_1^{-1}*g_2(s_2).$$

因而$\mathrm{Orb}(s_1)$的任意元素$g(s_1)$皆可写成

$$g(s_1)=g*g_1^{-1}*g_2(s_2)=g'(s_2)\in\mathrm{Orb}(s_2).$$

所以$\mathrm{Orb}(s_1)\subset\mathrm{Orb}(s_2)$。同理可证$\mathrm{Orb}(s_2)\subset\mathrm{Orb}(s_1)$。故

$$\mathrm{Orb}(s_1)=\mathrm{Orb}(s_2).\ \blacksquare$$

定义2.5 设群G为集合S的变换群，T为S的子集。如果对T的任意元素t及G的任意元素g，总有$g(t)$在T中，即

$$g(t)\in T,\quad \forall t\in T,\ g\in G,$$

则称T为一个(在G变换下的)**不变集合**。

不难看出，不变集合是一些轨道的并集。例如，在旋转群的作用下，平面上以旋转心为心的圆盘(即圆内点集)是不变集合。如果T为一个不变集合，则G可以理解成集合T上的变换群。

群G既然是集合T的变换群，则群G中的任意元素g都是T到自身的满射(见定理2.1)。于是定义2.5可改写成：

定义2.5* 设群G为集合S的变换群。设T为S的子集。如果对于G的任意元素g，总有

$$g(T)=T,$$

则称T为一个**不变集合**。

习　题

1．以V表示全体n维实向量的集合。$\mathrm{GL}(n,\boldsymbol{R})$在$V$上作用为左乘，即对于$A\in\mathrm{GL}(n,\boldsymbol{R})$及

$$a=\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix}\in V,$$

定义$A(a)=Aa$。试求所有轨道。

2．设$G=\mathrm{GL}(n,\boldsymbol{R})\times\mathrm{GL}(n,\boldsymbol{R})$。定义$G$在$\mathrm{FL}(n,\boldsymbol{R})$上的作用如下：对$(A,B)\in G$及$M\in\mathrm{FL}(n,\boldsymbol{R})$，令

$$(A,B)(M)=AMB^{-1}.$$

求所有轨道。

3. 以F表示所有$n\times n$实对称矩阵的集合。定义$\mathrm{GL}(n,\boldsymbol{R})$在$F$上的作用如下：对$S\in\mathrm{GL}(n,\boldsymbol{R})$，$A\in F$，令

$$S(A)=SAS^T,$$

其中S^T表示矩阵S的转置。求轨道的个数。

4. 令群G从左边作用在G上，即

$$g(g^*)=g\cdot g^*.$$

求$\mathrm{Orb}(g^*)$。

5. 令S_3从两边作用在S_3上，即

$$g(g^*)=gg^*g^{-1}.$$

求所有轨道。

6. 令$G=\boldsymbol{R}$。G通过下法作用在实平面$\boldsymbol{R}^2$上：对$r\in G$，

$$r((x,y))=(x+r,\ e^{-r}y),$$

试求所有轨道。

7. 圆环面T_2(torus)可以理解成下列的点集：

$$T_2=\{(a,b):0\leqslant a<1,\ 0\leqslant b<1\}.$$

令$G=\boldsymbol{R}$通过下法作用在T_2上：对$r\in\boldsymbol{R}$，令

$$r((a,b))=(a',b'),$$

其中$a'=a+r-[a+r]$，$b'=b+r-[b+r]$，$[a+r]$与$[b+r]$分别表示$a+r$和$b+r$的整数部分。试求所有轨道。

8. 参考上题。给定$c\in\boldsymbol{R}$，定义G在T_2上的作用为

$$r((a,b))=(a',b'),$$

其中$a'=a+cr-[a+cr]$，$b'=b+cr-[b+cr]$。讨论当c是有理数或无理数时轨道的不同性质。

9. 设G为S上的变换群。在S中定义关系"$\sim$"：$a\sim b\Longleftrightarrow a,b$属于同一轨道。证明"$\sim$"是一个等价关系，轨道则是关于$\sim$的等价类。

10. 在例6和例7中决定等价类(即轨道)的代表元素集合。

11. 在本节习题6,7,8中决定轨道的代表元素集合。

12. 令

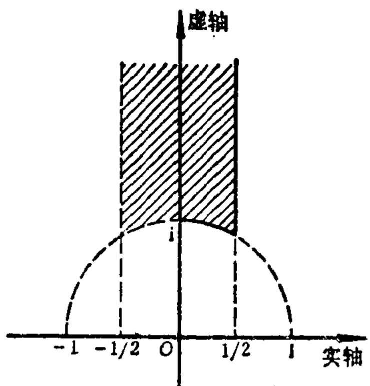
$$\mathrm{SL}(2,\boldsymbol{Z})=\left\{\begin{bmatrix}a & b\\ c & d\end{bmatrix}: a,b,c,d\in\boldsymbol{Z},\ \det\begin{bmatrix}a & b\\ c & d\end{bmatrix}=1\right\},$$

证明 SL(2, $\boldsymbol{Z}$)对矩阵乘法构成群。令H为上半复平面，即 $H=\{z: z\in\boldsymbol{C},\ \mathrm{Im}\, z>0\}$。

定义 SL(2, $\boldsymbol{Z}$)在H上的作用为

$$\begin{bmatrix}a & b\\ c & d\end{bmatrix}(z)=\frac{az+b}{cz+d}.$$

验证 SL(2, $\boldsymbol{Z}$)是H上的变换群。证明轨道的代表集合如图中斜线部分（斜线部分的以实线表示的边界在代表集合之中）。



题 12 图

§3 子　　群

在上一节中我们看到，如果群G是集合S上的变换群，则G对S所起的作用之一是把S划分成一些轨道及一些不变集合。那么，S对G所起的反作用是什么呢？为此，引入"子群"的概念。

定义2.6　设(G, $*$)为一群，H为G的一子集。如果(H, $*$)也为一群，则称H为G的**子群**，记为$H<G$。

讨论　要证明群G的一个非空子集H为一子群，只需要验证对于H中的任意二元素a及b，$a*b^{-1}$仍在H中即可。其理由如下：因为G中有结合律，故H中必有结合律；取$a=b$，则$e=a*a^{-1}\in H$，即H中有幺元；如果取$a=e$，则$e*b^{-1}=b^{-1}$，故H中任意元素b皆在H中有逆元素；以b^{-1}代替b，则有

$$a*b=a*(b^{-1})^{-1}\in H,$$

即H对$*$是封闭的。故H为一子群。

例 8 所有偶数是整数加群 $\mathbf{Z}$ 的一个子群，而所有奇数则不是 $\mathbf{Z}$ 的子群. 这因为两个奇数的差并不是奇数。偶数集合可写成 $2\mathbf{Z}$，由 2 及 -2（2 的加法逆元素）累次相加所构成。▌

一般而言，设 F 是群 $(G,*)$ 的一个子集，则所有形如 $a*b*\cdots*h$ 的元素构成一子群 H，其中 $a,b,\cdots,h$ 为 F 及 F^{-1}（即 F 中所有元素的逆元素构成的集合）中有限多个元素。如果 F 为空集，则此子群被理解为幺群。这个子群 H 被称为子集 F **生成的**，记为 $H=\langle F\rangle$。例如，$2\mathbf{Z}$ 是 $\{2\}$ 生成的。子集 F 称为子群 H 的**生成元集**。如果一个有限子集 F 可以生成群 G，则称群 G 是一个**有限生成的群**。

定义2.7 一个群 G 的基数（即 G 中元素的个数）称为群 G 的**阶数**，用 $o(G)$ 表示之。如果 $o(G)$ 为有限数，则称 G 为**有限群**；反之，则称 G 为**无限群**。元素 a 的**阶数** $o(a)$ 即其生成的子群的阶数。

例 9 平面上的旋转群的有限子群。

令原点为旋转心。设此子群 H 不为幺群。除去幺元后，令 ρ_θ 为其余的元素中具有最小的旋转角者。设 ρ_{θ_1} 为 H 中的任意元素。令 n 与 r 如下式所示：

$$n=[\theta_1/\theta],\qquad \theta_1=n\theta+r,$$

其中 $[\theta_1/\theta]$ 表示 θ_1/θ 的整数部分。则 $0\leqslant r<\theta$。于是

$$\rho_{\theta_1}*\rho_\theta^{-n}=\rho_{[\theta_1-n\theta]}=\rho_r.$$

但 θ 是最小旋转角，故 $r=0$。即 H 中的元素的旋转角皆为 θ 的倍数。令 m 为具有下述性质的整数：

$$m\theta\leqslant 360^\circ<(m+1)\theta.$$

则有

$$\rho_\theta^{m+1}=\rho_{[(m+1)\theta]}=\rho_{(m+1)\theta-360^\circ}.$$

根据以上讨论，知存在整数 s，使 $(m+1)\theta-360^\circ=s\theta$。易知

$$s=1,\qquad \theta=360^\circ/m.$$

不难看出，$m=o(H)$。如果 $m\geqslant 3$，则除原点外，任意点在

H 作用下的轨道皆为正 m 边形的 m 个顶点的集合。

定义2.8 设 G 为集合 S 的变换群。S 的一个子集 T 的**稳定群** Stab(T)定义为

$$\mathrm{Stab}(T)=\{g:\ g(T)=T\}.$$

讨论 Stab(T)为 G 的一个子群。事实上，由 $g(T)=T$，得

$$(g^{-1}*g)(T)=g^{-1}(T),\qquad e(T)=g^{-1}(T),\qquad T=g^{-1}(T),$$

即
$$g\in\mathrm{Stab}(T)\Longrightarrow g^{-1}\in\mathrm{Stab}(T).$$

又显然可见，对于 $g,h\in\mathrm{Stab}(T)$，有

$$(g*h)(T)=g(h(T))=g(T)=T,$$

故 $g*h$ 在 Stab(T)中。由此得知 Stab(T)为 G 的一个子群。∎

实际上，群 G 的任意子群皆可表示成一个稳定群。令群 G 如通常那样作用在集合 G 上，即

$$g(g_1)=g*g_1.$$

则 $\mathrm{Stab}(H)=H$。

我们可以将子群 H 视为集合 G 上的变换群（H 在 G 上的作用如前所示）。则有

$$\mathrm{Orb}(e)=\{h*e:\ h\in H\}=H.$$

此时的各条轨道 $\mathrm{Orb}(g)=\{h*g:\ h\in H\}$ 又称为**右陪集**。类似地，也有"左陪集"，其构造法如下：令子群 H 在集合 G 上的作用为

$$h(g)=g*h^{-1},\quad h\in H,\ g\in G.$$

则产生的轨道 $\{g*h^{-1}:\ h\in H\}=\{g*h:\ h\in H\}$ 称为**左陪集**。左、右陪集的性质很类似。在以下如果一般地用"**陪集**"这个词，而不特别指明是左、右陪集时，则皆指左陪集而言。

陪集既然是轨道，从定理2.2立得下面的系。

系 群 G 是对子群 H 的陪集的并集，并且这些陪集是分离的。

定理2.3 群 G 对于子群 H 的任意二陪集有相同的基数。

证明 只要证任意 $\mathrm{Orb}(g)=\{g*h:\ h\in H\}$ 与 $\mathrm{Orb}(e)=H$ 有相同的基数即可。定义由 H 到 Orb(g)的映射 g^*：

$$g^*(h) = g * h, \quad h \in H.$$

显然此映射是既单又满的，故H与$\mathrm{Orb}(g)$基数相同。▎

定义2.9 一子群H对群G的指数定义为G对H的陪集的集合的基数，即陪集的数目，记为$[G:H]$。

从定理2.3及定义2.9，我们立得如下的**拉格朗日定理**：

定理2.4 如G为有限群，而H为G的子群，则

$$o(G) = [G:H] \cdot o(H).$$

下面的定理可以阐明"指数"的意义。

定理2.5 设群G为集合S的变换群，T为集合S的子集，$\mathrm{Stab}(T)$为T的稳定群。则在G的作用下所产生的不同的$g(T)$的数目等于指数$[G:\mathrm{Stab}(T)]$，此处g是G的元素。

证明 任意取G的二元素g_1, g_2。我们若能证明：

$$g_1(T) = g_2(T)$$

当且仅当g_1和g_2属于G对$\mathrm{Stab}(T)$的同一陪集，定理即得证。

记$\mathrm{Stab}(T) = H$。如$g_1, g_2 \in g * H$，即存在$h_1, h_2 \in H$，使得

$$g_1 = g * h_1, \qquad g_2 = g * h_2,$$

则有

$$g_1(T) = g(h_1(T)) = g(T) = g(h_2(T)) = g_2(T).$$

反之，若$g_1(T) = g_2(T)$，则

$$g_2^{-1} * g_1(T) = g_2^{-1} * g_2(T) = e(T) = T,$$

即$g_2^{-1} * g_1 \in H = \mathrm{Stab}(T)$，也即$g_1 \in g_2 H$。故$g_1, g_2$属于同一陪集。▎

在上面的定理中，取$S = G$，$T = H (H < G)$，则显然有

$$\mathrm{Stab}(H) = H.$$

不同的$g(H) = g * H$的数目自然是$[G:H]$（参见定义2.9）。

在下面的例子中，我们要用定理2.5去完成一些有趣的计算。

例 10 三维实空间的有限旋转群。此群可以应用到晶体群上。

取幺球面S，即以原点为心，半径为1的球面。设原点为此

有限旋转群G的所有元素的共同旋转心，则G作用在S上，成为S的变换群。G中非幺的元素ρ在三维实空间中必有一旋转轴，即ρ在S上有两个极点(在ρ下保持不动的点)。

设P为S上一点，以ν_P表示$\mathrm{Orb}(P)$的基数。令

$$n_P=o(\mathrm{Stab}(P)),\qquad n=o(G),$$

由定理2.5，有$\nu_P=[G:\mathrm{Stab}(P)]$，故

$$n=n_P\cdot\nu_P.$$

既然每一个非幺的旋转皆有两极，在重复计算下，G中全体非幺元素总共应有$2(n-1)$个极点。注意到以P为极点的非幺旋转的集合恰是$\mathrm{Stab}(P)\backslash\{e\}$($e$为幺旋转)，故$P$点作为极点的重复次数为$n_P-1$。再注意到$\mathrm{Orb}(P)$中的点都是极点，而且这些极点的重复次数都是$n_P-1$，故有

$$2(n-1)=\sum_i\nu_{P_i}(n_{P_i}-1)=\sum_i(n-\nu_{P_i}).$$

上式中的求和含意如下：在每个轨道中取定一个P_i，然后关于所有的P_i求和(故求和式的项数即为轨道的个数)。把上式除以n，则得

$$(1)\qquad 2-\frac{2}{n}=\sum_i\left(1-\frac{\nu_{P_i}}{n}\right)=\sum_i\left(1-\frac{1}{n_{P_i}}\right).$$

由于P_i为某一非幺旋转的极点，故$\mathrm{Stab}(P_i)$必非幺群。所以

$$n_{P_i}=o(\mathrm{Stab}(P_i))\geqslant 2,$$

即

$$1-\frac{1}{n_{P_i}}\geqslant\frac{1}{2}.$$

由此即知所有极点最多只能划分成三个不同的轨道。我们将罗列所有的可能性如下(由(1)式易知不可能只有一条轨道)。

1) 所有极点归入两条轨道。此时(1)式化为

$$2-\frac{2}{n}=\left(1-\frac{1}{n_{P_1}}\right)+\left(1-\frac{1}{n_{P_2}}\right),$$

即有

$$\frac{2}{n}=\frac{1}{n_{P_1}}+\frac{1}{n_{P_2}},$$

故得

$$n=n_{P_1}=n_{P_2}, \quad 1=\nu_{P_1}=\nu_{P_2}.$$

即所有旋转皆保持 P_1, P_2 不动。换言之，P_1 及 P_2 是此旋转群的共用的南北极。此群必然是赤道平面上的旋转所引生的（参见例9）。

2）所有极点归入三个轨道。最小的 n_{P_i} 必然为2。设有两个 n_{P_i} 为 2，则可由(1)式解得

$$n_{P_1}=n_{P_2}=2, \quad n_{P_3}=n/2.$$

故

$$\nu_{P_1}=\nu_{P_2}=n/2=n_{P_3}, \quad \nu_{P_3}=2.$$

不难看出，这个旋转群是由过原点的一个平面（不妨令为 X-Y 平面）累次旋转 $360°/n_{P_3}$ 及以此平面上过 P_1 的直线（不妨令为 X 轴）为轴的180°的旋转所产生的，也即图2.3中的多面体的旋转群。P_2 为 X-Y 平面上正 n_{P_3} 边形一边的中点在幺球面上的投影。

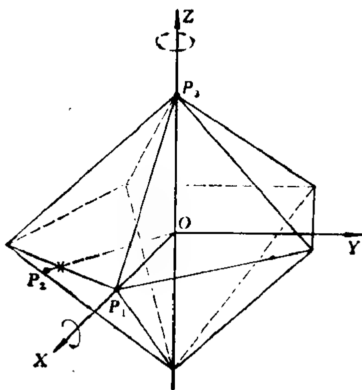


图 2.3

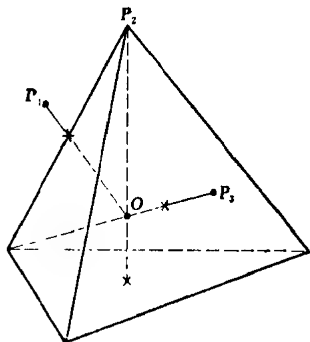


图 2.4

3）所有极点归入三个轨道，最小的n_{P_1}是2，次小者为3。由(1)式可解得

$$n_{P_1}=2,\quad n_{P_2}=3,\quad \frac{1}{n_{P_3}}=\frac{1}{6}+\frac{2}{n}.$$

此时又有以下三种可能：

(a) $n_{P_1}=2,\quad n_{P_2}=3,\quad n_{P_3}=3,\quad n=12.$

于是有$\nu_{P_1}=6$，$\nu_{P_2}=4$，$\nu_{P_3}=4$。如取P_2轨道中的4个点，则成为一正金字塔形的四个顶点(图2.4)。P_1是一边中点在幺球面上的投影。因为有六条边，故P_1的轨道中有六个点。P_3是一个面的中心在幺球面上的投影，因为有四个面，故P_3的轨道中有四点。G即是此正四面体的变换群。

(b) $n_{P_1}=2,\quad n_{P_2}=3,\quad n_{P_3}=4,\quad n=24.$

于是有

$$\nu_{P_1}=12,\quad \nu_{P_2}=8,\quad \nu_{P_3}=6.$$

如取P_2的轨道中的八个点为顶点，则成一正六面体。如取P_3的轨道中的六点为顶点，则成一正八面体(图2.5)。群G是此两种正多面体的变换群。其余各极点是边与面的中点在幺球面上的投

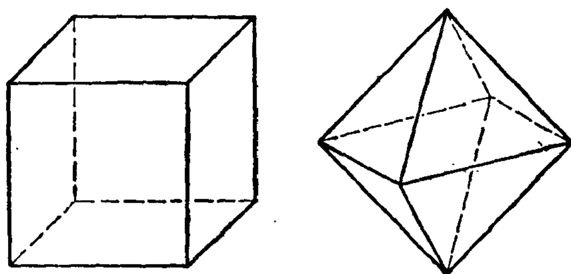


图 2.5

影。这两种正多面体是“共轭”的，即连接其中之一的各面的中心就能得出另一正多面体。故两者的旋转群是相同的。

(c) $n_{P_1}=2$, $n_{P_2}=3$, $n_{P_3}=5$, $n=60$.

于是有 $\nu_{P_1}=30$，$\nu_{P_2}=20$，$\nu_{P_3}=12$。与以上的讨论类似，我们可以得出此时群G是正十二面体与正二十面体的旋转群（图2.6）。▌

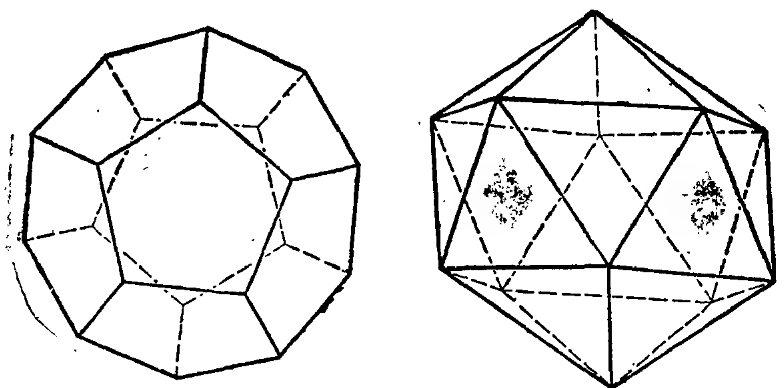


图 2.6

以上得出三维空间的全部有限旋转群。可堪注意的是，自古希腊便知道仅有五种正多面体，而(a)，(b)，(c)正好得出三个不同的群，分别是这些正多面体的旋转群。

习 题

1. 证明群G的任意多个子群的交仍为G的子群；设H_1，$H_2<G$，证明$(H_1\cup H_2)<G\Longleftrightarrow H_1\subset H_2$或$H_1\supset H_2$；令

$$H_1*H_2=\{h_1*h_2:\ h_1\in H_1,\ h_2\in H_2\}.$$

举例说明H_1*H_2不一定是G的子群。

2. 设$H<G$，证明对任一$g\in G$，$gHg^{-1}<G$。

3. 设$S\subset G$。定义

$$C(S)=\{x:\ x\in G,\ xs=sx(\forall s\in S)\}.$$

证明$C(S)<G$（$C(S)$称为S在G中的中心化子）。

4. 设$S\subset G$。定义

$$N(S)=\{x: x\in G,\ xS=Sx\}.$$

证明$N(S)<G$ ($N(S)$称为S在G中的正规化子)。

5. 设G为有限群. 证明对于任一$g\in G$, $g^{o(G)}=e$。

6. 设G是n阶循环群, $m|n$. 证明G有且只有一个m阶子群。

7. 设G为循环群, $g\in G$, s,t为正整数。证明

(1) $\langle a^s\rangle\cap\langle a^t\rangle=\langle a^{[s,t]}\rangle$, 此处$[s,t]$表示$s$和$t$的最小公倍数;

(2) $\langle a^s\rangle\cdot\langle a^t\rangle<G$, 且$\langle a^s\rangle\langle a^t\rangle=\langle a^{(s,t)}\rangle$, 此处$(s,t)$表示$s$和$t$的最大公因数。

8. 考虑$\mathrm{GL}(2,\boldsymbol{R})$。取

$$g_1=\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix},\qquad g_2=\begin{bmatrix}0 & 1\\ -1 & -1\end{bmatrix}.$$

证明$o(g_1)=4$, $o(g_2)=3$, $o(g_1\cdot g_2)=\infty$。

9. 设G是群. 令G'为G的换位子群 (commutator subgroup), 即G中所有形如$g_1^{-1}g_2^{-1}g_1g_2$的元素生成的子群(g_1, $g_2\in G$)。证明对于任一$g\in G$, 都有$gG'=G'g$。

10. 令

$$O_+(n,\boldsymbol{R})=\{A: A\in\mathrm{GL}(n,\boldsymbol{R}),\ A^TA=E,\ \det A=1\},$$

其中E表示n阶单位方阵. $O_+(n,\boldsymbol{R})$的元素可以理解成由它的行向量决定的正交座标系。证明$O_+(n,\boldsymbol{R})$中任一元素对$O_+(n-1,\boldsymbol{R})$的左陪集可以自然地理解成n维球面S^n。

11. 令$\boldsymbol{P}_C^1=\boldsymbol{C}\cup\{\infty\}$, 令$G$为$\boldsymbol{P}_C^1$的线性变换群, 即

$$G=\left\{Z\to\frac{az+b}{cz+d}(\forall z\in\boldsymbol{P}_C^1): a,b,c,d\in\boldsymbol{C},\right.$$

$$\left.\det\begin{bmatrix}a & b\\ c & d\end{bmatrix}\neq 0\right\}.$$

令 $T=\{0,1,\infty\}\subset \boldsymbol{P}_{C}^{1}$，求 $\mathrm{Stab}(T)$。

12. 令 G 为平面 $\boldsymbol{R}^2$ 的平移群，求 $\mathrm{Stab}(\boldsymbol{Z}\times\boldsymbol{Z})$。

13. 设 G 是一个交换群。如果 G 的每一个真子群都是有限群，G 是否必然为有限群？

14. 设 G 是群，$H_1,H_2,\cdots,H_n<G$，且 $[G:H_i]<\infty$（$\forall i=1,2,\cdots,n$）。证明 $\left[G:\bigcap\limits_{i=1}^{n}H_i\right]<\infty$。

15. 有限生成群的子群是否必为有限生成的？

16. 证明有限生成群的指数有限的子群必为有限生成的。

17. 完成例10 的 3)中(c)的讨论。

18. 找一个非交换群，使它的每一个真子群都是交换群。

§4 内自同构及正规子群

在上节中我们讨论左、右陪集时，曾用两种不同的方法使群 G 作用在集合 G 上。这两种作用带来了一些结果。在本节中，我们将引入另一种作用。

设 g 为群 G 的一个元素。令 g 作用在集合 G 上如下：

$$g(g_1)=g*g_1*g^{-1},\qquad \forall g_1\in G.$$

这一作用所造成的 G 到自身的映射称为 g 所引生的**内自同构**，记为 τ_g。为了阐明"内自同构"这一名词的意义，请注意 τ_g 的如下的性质：

$$\begin{aligned}\tau_g(g_1*g_2)&=g(g_1*g_2)=g*g_1*g_2*g^{-1}\\&=g*g_1*g^{-1}*g*g_2*g^{-1}\\&=\tau(g_1)*\tau(g_2),\end{aligned}$$

并把此性质与下面的两个定义相比较。

定义2.10 设 $\rho: G\to G'$ 为群 G 到群 G' 的一个映射。如果 ρ 保持群的运算关系，即

$$\rho(g_1*g_2)=\rho(g_1)*\rho(g_2),\qquad \forall g_1,g_2\in G,$$

则称 ρ 为 G 到 G' 内的一群映射（或同态）。

定义2.11 设 ρ 为群 G 到群 G' 内的一个群映射。如果 ρ 为单射，则称 ρ 为**群单射**；如 ρ 为满射，则称 ρ 为**群满射**，此时称 G 和 G' 为**同态**。如果 ρ 为单满映射，则称 ρ 为**同构**，记为 ρ: $G\approx G'$。如果 ρ 为同构且为 G 到自身的映射，即 $G'=G$，则称 ρ 为**自同构**。

讨论 1）不难看出"内自同构" τ_g 是一个群映射，并且 τ_g 适合下列的公式：

$$\begin{aligned}g_1(g_2(g_3)) &= \tau_{g_1}(\tau_{g_2}(g_3)) = \tau_{g_1}(g_2 * g_3 * g_2^{-1})\\&= g_1 * g_2 * g_3 * g_2^{-1} * g_1^{-1} = (g_1 * g_2) * g_3 * (g_1 * g_2)^{-1}\\&= \tau_{g_1 * g_2}(g_3) = (g_1 * g_2)(g_3),\end{aligned}$$

$$e(g_3) = \tau_e(g_3) = e * g_3 * e^{-1} = g_3.$$

故群 G 以内自同构作用于集合 G 上，构成集合 G 的变换群。根据定理2.1，即知所有内自同构 τ_g 都是集合 G 到自身的单满映射，所以皆是自同构。这种由 G "内"的元素所引生的自同构，自然称为内自同构。

如此作用下产生的轨道，称为**共轭类**。如果二元素 g_1 及 g_2 属于同一共轭类，则称 g_1 与 g_2 **共轭**，即有一 g，使得

$$g * g_1 * g^{-1} = g_2.$$

2）因为

$$\rho(e) * \rho(g) = \rho(e * g) = \rho(g),$$

故 $e'=\rho(e)$ 是 G' 的幺元。又有

$$\rho(g) * \rho(g^{-1}) = \rho(g * g^{-1}) = \rho(e) = e',$$

故知 $\rho(g^{-1}) = \rho(g)^{-1}$。

定义2.12 令群 G 通过内自同构作用在集合 G 上。G 的**不变子群** H，即同时为子群及不变集合者，称为 G 的**正规子群**，记为 $G\rhd H$。群 G 中轨道为幺集（即只含有一个元素的集合）者的并集，称为群的**心**。

讨论 1）正规子群 H 就是适合下式的子群：

$$g*H*g^{-1}=H,\quad \forall g\in G.$$

2) 如果 g 的轨道是幺集，则必有

$$\tau_{g_1}(g)=g_1*g*g_1^{-1}=g,$$

即

$$g_1*g=g*g_1,\quad \forall g_1\in G.$$

换言之，即 g 与群 G 中的任意元素 g_1 进行运算时可以交换。这是 g 在群的心中的充要条件。

定义2.13 如果群 G 的心就是群 G 本身，换言之，我们有

$$g_1*g_2=g_2*g_1,\quad \forall g_1,g_2\in G,$$

即运算的交换律成立，则称 G 为**交换群**。反之，则称为**非交换群**。

例11 §1 例 1 中的群皆是交换群。例 3 中的平面的平移群、反射群，以及旋转群也皆是交换群，而刚体运动群则是非交换群。▌

对于群 G 的心，我们还有另外一种理解方法，即 g 在群 G 的心中的充要条件是

$$\tau_g(g_1)=g_1,\quad \forall g_1\in G.$$

换言之，即 g 所引生的内自同构是幺映射。一般言之，我们有如下的定理。

定理2.6 设群 G 为集合 S 的变换群。则 G 中等同于 S 的幺映射的元素的集合构成 G 的一个正规子群。

证明 设此集合为 H。显然，$e\in H$，故 H 非空。设 $a,b\in H$，则

$$a*b^{-1}(s)=a(b^{-1}(s))=a(s)=s,\quad \forall s\in S.$$

故知 H 为一子群。令 g 为 G 的任意元素，则有

$$\begin{aligned}\tau_g(a)(s)&=(g*a*g^{-1})(s)=g(a(g^{-1}(s)))\\&=g(g^{-1}(s))=g*g^{-1}(s)=e(s)=s,\quad \forall s\in S.\end{aligned}$$

故知 $\tau_g(a)\in H$。根据定义 2.5，即知H为不变子集。于是H为一正规子群。❙

系　群的心是一个正规子群。

以后我们还会讨论定理 2.6。目前我们继续研究与正规子群有关的题材。

定义2.14　设 ρ 为群G到群G'的一个群映射。ρ 的**象** $\mathrm{im}(\rho)$ 的定义如下：

$$\mathrm{im}(\rho)=\{g': \text{存在 } g\in G,\ \text{使得 } \rho(g)=g'\};$$

ρ 的**核**的定义如下：

$$\ker(\rho)=\{g: \rho(g)=e',\ e' \text{ 为 } G' \text{ 的幺元}\}.$$

换言之，$\ker(\rho)$即是 e' 在 ρ 作用下的**象源**，故也可以用 $\rho^{-1}(e')$ 表示之。

定理2.7　设 ρ 为群G到群G'的一个群映射，则 $\mathrm{im}(\rho)$是G'的子群。如果H'是 $\mathrm{im}(\rho)$的一个(正规)子群，则H'的象源H(即 $H=\{g: \rho(g)\in H\}$)是G的(正规)子群。

证明　设 $g_1',g_2'\in\mathrm{im}(\rho)$，则存在 $g_1,g_2\in G$，使得

$$\rho(g_1)=g_1',\quad \rho(g_2)=g_2'.$$

于是有

$$\begin{aligned}\rho(g_1*g_2^{-1})&=\rho(g_1)*\rho(g_2^{-1})=\rho(g_1)*\rho(g_2)^{-1}\\&=g_1'*(g_2')^{-1},\end{aligned}$$

即 $g_1'*(g_2')^{-1}\in\mathrm{im}(\rho)$。因 $e'=\rho(e)\in\mathrm{im}(\rho)$，故 $\mathrm{im}(\rho)$非空，故知 $\mathrm{im}(\rho)$为G'的一个子群。

显然，$\rho(e)=e'\in H'$，故 $e\in H$，即H非空。令 $g_1,g_2\in H$，则

$$\begin{aligned}\rho(g_1*g_2^{-1})&=\rho(g_1)*\rho(g_2^{-1})\\&=\rho(g_1)*\rho(g_2)^{-1}\in H',\end{aligned}$$

故 $g_1*g_2^{-1}\in H$。于是H是G的子群。

现设H'为 $\mathrm{im}(\rho)$的正规子群。令 τ_g 为G的任一内自同构，

则对于任一 $g_1 \in H$，有

$$\rho(\tau_g(g_1)) = \rho(g * g_1 * g^{-1})$$
$$= (\rho(g) * \rho(g_1)) * \rho(g)^{-1}.$$

由于 H' 为 $\mathrm{im}(\rho)$的正规子群，故 $\rho(g) * H' * \rho(g)^{-1} = H'$， 即

$$\rho(g) * H' = H' * \rho(g).$$

而 $\rho(g_1) \in H'$，故存在 $h' \in H'$，使得

$$\rho(g) * \rho(g_1) = h' * \rho(g).$$

代入上式，即有

$$\rho(\tau_g(g_1)) = (h' * \rho(g)) * \rho(g)^{-1} = h' * \rho(g * g^{-1}) = h'.$$

故得 $\tau_g(g_1) \in H$，即H为G的不变子集。由此得知H为G的正规子群。▌

系 设 ρ 为群G到G'的群映射，则 $\ker(\rho)$ 是群G的正规子群。

以上我们证明了许多子群是正规子群。正规子群的重要意义在于下面的定理。

定理2.8 设H为G的正规子群。如果在G对H的陪集的集合$\{g * H: g \in G\}$中引入如下的自然运算：

$$(g_1 * H) * (g_2 * H) = (g_1 * g_2) * H,$$

则此陪集的集合成为一群，称之为G对H的**商群**，记为G/H。

证明 我们首先要证明此定理中引入的自然运算是有意义的。换言之，如果

$$g_1 * H = g_3 * H, \quad g_2 * H = g_4 * H,$$

则应有

$$(g_1 * g_2) * H = (g_3 * g_4) * H.$$

即 $g_1 * g_2$ 与 $g_3 * g_4$ 应属于同一陪集。事实上，设 $h_1, h_2 \in H$，使得 $g_1 = g_3 * h_1$，$g_2 = g_4 * h_2$，则

$$g_1 * g_2 = g_3 * (h_1 * g_4) * h_2.$$

因为H为正规子群，所以有 $h_3 \in H$，使得 $h_1 * g_4 = g_4 * h_3$，故

$$g_1 * g_2 = g_3 * g_4 * h_3 * h_2.$$

即 $g_1 * g_2$ 与 $g_3 * g_4$ 属于同一个陪集。

不难看出，运算的结合律继续有效，$e * H = H$ 是幺元，$g * H$ 的逆元素是 $g^{-1} * H$。故 G/H 是一群。 ▍

以下我们将证明的定理，通常称为**第一同构定理**。

定理2.9 设 ρ 为群 G 到群 G' 的群满射。令 H' 为 G' 的一个正规子群，H 为 H' 的象源。则如下定义的 $\bar{\rho}$：

$$\bar{\rho}(g * H) = \rho(g) * H'$$

是商群 G/H 到商群 G'/H' 的一个同构。

证明 首先，我们必须证明如此定义的 $\bar{\rho}$ 是有意义的。换言之，如果 $g_1 * H = g_2 * H$，则应有 $\rho(g_1) * H' = \rho(g_2) * H'$。事实上，由于 g_1 及 g_2 属于同一陪集，即 $g_1^{-1} * g_2 \in H$，故

$$\rho(g_1)^{-1} * \rho(g_2) = \rho(g_1^{-1} * g_2) \in H',$$

即 $\rho(g_1)$ 与 $\rho(g_2)$ 属于对 H' 的同一陪集。此即须证之点。

其次，我们要证 $\bar{\rho}$ 是群映射。令 $g_1, g_2 \in G$，则有

$$\begin{aligned}\bar{\rho}((g_1 * H) * (g_2 * H)) &= \bar{\rho}(g_1 * g_2 * H) = \rho(g_1 * g_2) * H' \\ &= \rho(g_1) * \rho(g_2) * H' = (\rho(g_1) * H') * (\rho(g_2) * H') \\ &= \bar{\rho}(g_1 * H) * \bar{\rho}(g_2 * H).\end{aligned}$$

故知 $\bar{\rho}$ 为群映射。

取 $g' * H'$ 为商群 G'/H' 中之任意元素。因为 ρ 为满射，所以在 G 中存在 g，使得 $\rho(g) = g'$。故有

$$\bar{\rho}(g * H) = \rho(g) * H' = g' * H',$$

所以 $\bar{\rho}$ 是满射。

若 $\bar{\rho}(g_1 * H) = \bar{\rho}(g_2 * H)$，则 $\rho(g_1) * H' = \rho(g_2) * H'$。即

$$\rho(g_1^{-1} * g_2) = \rho(g_1)^{-1} * \rho(g_2) \in H'.$$

H 既然是 H' 的象源，故 $g_1^{-1} * g_2 \in H$，即 $g_1 * H = g_2 * H$。由此得知 $\bar{\rho}$ 为单射。故 $\bar{\rho}$ 为同构。 ▍

系 设 ρ 为群 G 到群 G' 的群映射，则 $G/\ker(\rho)$ 与 $\mathrm{im}(\rho)$ 同构。

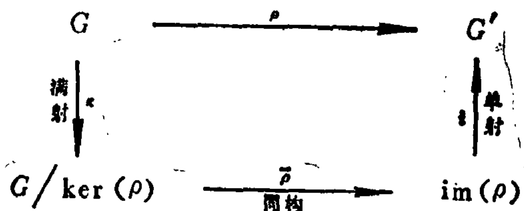
定义2.15 设 H 为群 G 的正规子群。则群 G 到商群 G/H 的

典型映射 κ 的定义如下：

$$\kappa(g)=g*H,\quad \forall g\in G.$$

讨论 不难看出，典型映射是一个群满射。

根据定理2.9的系及定义2.15，任意的群映射 $\rho: G\to G'$ 皆可分解成下列三个映射的合成：



其中 $\iota(g')=g'$ 为群单射；$\rho=\iota\circ\bar{\rho}\circ\kappa$。

例12 对称群 S_n 的轨道式及共轭类。

设 $\sigma\in S_n$。取在 σ 生成的子群 $\langle\sigma\rangle$ 作用下的任意一条轨道及此轨中的任一数字 i，则可把这条轨道写成下式：

$$(i,\sigma(i),\cdots,\sigma^{l-1}(i)),$$

其中的数字 $\sigma(i),\cdots,\sigma^{l-1}(i)$ 皆不同于 i，而 $\sigma^l(i)=i$。把 $\langle\sigma\rangle$ 作用下的所有轨道罗列起来，则得 σ 的轨道式如下：

$$(i,\sigma(i),\cdots)(j,\sigma(j),\cdots)(k,\sigma(k),\cdots).$$

上面的轨道式中，各轨道的先后次序是无关紧要的。一般地，在上式中如果某轨道仅有一个数字，则通常略去不写。显然，任一种上面的写法，只要不同的括号中不出现相同的数字，就必是 S_n 中某元素的轨道式。

对于 S_n 中的元素，有另外两种不同的理解法。其一是理解为位置的调换，其二是在位置上填写数字。例如，对 $\rho=(1,2,3)\in S_3$，既可以理解为把1号位置换成2号位置，2号换成3号，3号换成1号，也可以理解成在1号位置上填写数字2等等。我们不妨把第一种理解法写成

$$\rho(1)=2,\quad \rho(2)=3,\quad \rho(3)=1,$$

而把第二种理解法写成

$$1_\rho=2,\quad 2_\rho=3,\quad 3_\rho=1.$$

现设 $1\leqslant i\leqslant n$，$\sigma\in S_n$，τ_ρ 为由 ρ 引起的 S_n 的内自同构。则有

$$\tau_\rho(\sigma)(i_\rho)=\rho*\sigma*\rho^{-1}(\rho(i))=\rho*\sigma(i)=\sigma(i)_\rho.$$

如果把上式中的 σ 理解成调换位置，ρ 理解为填写数字，则上式可以理解成：$\tau_\rho(\sigma)$作用在 i 位上填写的数字 i_ρ 的结果，等于在 $\sigma(i)$位上应当填写的数字 $\sigma(i)_\rho$。这种说明似嫌罗嗦，我们且举一例：令 $\sigma=(1,2)$，$\rho=(1,2,3)$，则有 $\tau_\rho(\sigma)=(2,3)$。即在 σ 的轨道式中，按照 ρ 给定的规则，凡遇 1 号，则填上 2， 2 号填上 3，3 号填上 1，则得到 $\tau_\rho(\sigma)$。同法，例如 $\sigma_1=(2,4)(1,5)$，则 $\tau_\rho(\sigma_1)=(3,4)(2,5)$。

简言之，$\tau_\rho(\sigma)$即是将 σ 的轨道式中的数字全部按照 ρ 加以变换。由此得知，S_n 的两个元素属于同一共轭类的充要条件是它们的轨道式的形状相同。例如$(1,2)(3,4,5)$与任意元素$(a,b)(c,d,e)$共轭。自然，此式必须是一个轨道式，即五个数字 a,b,c,d,e 两两不同。

例13 如果 $n\neq2$，g 为 S_n 的非幺元素，则 g 引起的内自同构 τ_g 必不是幺映射。换言之，如果 $n\neq2$，则 S_n 的心是幺群。我们来证明这个事实。

在例12中，我们已经阐明内自同构 τ_ρ 的作用就是将 σ 的轨道式中的数字全部按照 ρ 加以变换。当 $n=1$ 时，无可证之事。设 $n\geqslant3$，而且 $\rho\neq e$(e 为 S_n 的幺元)。设

$$\rho=(i,j,\cdots)\cdots(\cdots),$$

取一数字 $k\neq i,j$，$1\leqslant k\leqslant n$。令 $\sigma=(i,k)$，则有

$$\tau_\rho(\sigma)=(j,s)\neq\sigma,$$

其中 $s=\rho(k)$，故知 τ_ρ 不是幺映射。

例14 我们取"人类学"的例子。据人类学家的研究，许多

原始社会的婚姻遵守下列几条通则：

通则一：全社会的人分成几类，同类的男女才可结为夫妻，不同类的男女的婚姻被视为禁忌；

通则二：一个人的类别是由父母的类别及其本人的性别决定的，反之，父母的类别也是由此人的类别决定的；

通则三：兄妹(或姐弟)的类别一定不同；

通则四：有亲属关系的两个人，其类别的异同仅由两个人的亲属关系决定，这在全社会中是一致的。例如，表兄妹的类别，可以是全社会一致地相同，或一致地相异；

通则五：任何两个人的后裔不可能世世不能结婚。

我们用群论的概念来研究这些婚姻通则。令社会中人的全部类别为$\{1,2,\cdots,n\}$。由父母传给子及女的类别的规律，根据通则二，是$\{1,2,\cdots,n\}$上的两个变换$S,D\in S_n$，即

$$S(i)=\text{当父母为 } i \text{ 类时儿子的类别},$$
$$D(i)=\text{当父母为 } i \text{ 类时女儿的类别}.$$

于是，通则三即

通则三′：$S(i)\neq D(i)$，$\forall i=1,2,\cdots,n$，即

$$DS^{-1}(i)\neq i,\quad \forall i=1,2,\cdots,n.$$

任何亲属关系，用追溯共同祖先的办法，可以写成S与D生成的子群$\langle S,D\rangle$中的一个元素。例如，堂兄妹(或堂弟姐)之间的关系即“父亲的父亲的儿子的女儿”，可写成

$$DSS^{-1}S^{-1}=DS^{-1},$$

于是根据通则三′，堂兄妹(或堂弟姐)的类别必不同，其婚姻是不允许的。又例如表兄妹(或表弟姐)的关系是“母亲的父亲的儿子的女儿”，可写成$DSD^{-1}S^{-1}$。于是通则四可以写成

通则四′：任取子群$\langle S,D\rangle$的元素M，如果$M\neq I$（I表示幺元），则有

$$M(i)\neq i,\quad \forall i=1,2,\cdots,n.$$

于是表兄妹可以成婚的数学式为

$$DSD^{-1}S^{-1}=I, \quad DS=SD,$$

即$\langle S,D\rangle$是一个交换群。

不难看出，通则五即下面的通则五′：

通则五′：在子群$\langle S,D\rangle$的作用下，任意 $i(1\leqslant i\leqslant n)$ 的轨道皆是整个集合$\{1,2,\cdots,n\}$。

于是，关于这些原始社会的婚姻规则的研究就可化为群论的某些问题。

我们试取 $n=4$，即此社会有四种不同类别的人。如果我们忽视数字的调换及重排，以及 S 与 D 的互换，则不难看出仅有如下的可能（令 $P=(1,2,3,4)$，I 为幺元）：

1) $S=P$, $D=I$;

2) $S=P$, $D=P^2$;

3) $S=P$, $D=P^3$;

4) $S=(1,2)(3,4)$, $D=(1,3)(2,4)$.

塔若(Tarau)人用 1)(实际上是 $S=I$，$D=P$)，凯瑞那 (Kariera) 人用 4)。易于证出，以上的四种形态中，$\langle S,D\rangle$恒为交换群，即社会中有四种类别时，表兄妹恒可成婚。

读者可以研究 $n=5$——即有五种类别——的情形。

习　题

1. 参考 §3 习题 4。设G为群，$A<G$，证明 $A\lhd N(A)$。

2. 举例说明一个群G的正规子群的正规子群不一定是G的正规子群。

3. 平面的平移群是不是平面的刚体运动群的正规子群？

4. 设 $H<G$，且$[G:H]=2$，证明 $H\lhd G$。

5. (1) 设 $H<G$，$g\in G$，证明 $g*H*g^{-1}<G$。特别地，如果 $H<G$，则 $g*H*g^{-1}\lhd G$。

(2) 设H是G的唯一的指数为 n 的子群，证明 $H\lhd G$。

6. 找出平面刚体运动群的心。

7. 令群 G 作用在集合 S 上。设 $b\in \mathrm{Orb}(a)$，证明 $\mathrm{Stab}(a)$ 与 $\mathrm{Stab}(b)$ 共轭。

8. 证明加群 $\boldsymbol{R}/\boldsymbol{Z}$ 与乘群 $C^1=\{e^{ix}: x\in \boldsymbol{R}\}\subset \boldsymbol{C}$ 同构。

9. 圆环面可以定义为 $\boldsymbol{R}^2/\boldsymbol{Z}\times \boldsymbol{Z}$。证明圆环面是一个加群。

10. 参考§3习题9。设 $G\rhd H$，证明

$$G/H \text{ 是交换群} \Longleftrightarrow H\supset G'.$$

11. 证明任何一个有限群 G 都与 S_n 的一个子群同构，此处 $n\geqslant o(G)$。

12. 设 p 是素数。$\boldsymbol{Z}/p^3\boldsymbol{Z}\oplus \boldsymbol{Z}/p^2\boldsymbol{Z}$ 有多少个阶为 p^2 的循环子群？

13. 从 $\boldsymbol{Z}/n\boldsymbol{Z}$ 到 $\boldsymbol{Z}/m\boldsymbol{Z}$ 有多少个群映射？

14. 研究例14中 $n=5$ 的情形。

§5 自同构群

在上节中我们研究了内自同构在群上的作用。如果群 G 是一个交换群，则所有的内自同构的作用皆同于群 G 的幺映射，这时的内自同构只不过具有表面上的复杂性而已，其本质非常简单。为了消除这种表面上的复杂性，我们引入如下的定义及定理。

定义2.16 设群 G 是集合 S 的变换群。如果只有 G 的幺元 e 是 S 的幺映射，则称 G 的作用是**忠实的**，否则就称为是**非忠实的**。

上节的定理2.6已证 G 中等同于 S 的幺映射的元素的集合是 G 的一个正规子群。我们有如下的定理。

定理2.10 设群 G 是集合 S 的变换群。令 H 为 G 中等同于 S 的幺映射的元素的集合，则 G/H 通过如下定义的在 S 上的作用，成为 S 的变换群，而且这个作用是忠实的：

$$(g*H)(s)=g(s),\quad \forall s\in S.$$

证明 首先，我们必须证明这个作用的定义是有意义的，即如果 $g_1 * H = g_2 * H$，则应有 $g_1(s) = g_2(s)$。事实上，此时存在 $h \in H$，使得 $g_1 = g_2 * h$，故

$$g_1(s) = (g_2 * h)(s) = g_2(h(s)) = g_2(s).$$

所以我们定义的作用是有意义的。不难看出

$$H(s) = s,$$

$$((g_1 * H) * (g_2 * H))(s) = (g_1 * g_2 * H)(s) = (g_1 * g_2)(s)$$
$$= g_1(g_2(s)) = (g_1 * H)((g_2 * H)(s)),$$

故知 G/H 是集合 S 的一个变换群。设 $g * H$ 在 S 上的作用等同于 S 的幺映射，则

$$g(s) = (g * H)(s) = s, \quad \forall s \in S,$$

故 g 在 H 中，换言之，$g * H = H$ 是 G/H 的幺元。 ▌

从代数的观点考虑，一个群 S 上的映射应当照顾其代数的运算关系，也即应该考虑群映射。

定义2.17 设 S 为一群。如果群 G 是集合 S 的变换群，且群 G 的元素都是群 S 的群映射，则称群 G 是群 S 的**变换群**。

讨论 根据定理 2.1，群 S 的变换群 G 中的元素皆为群 S 的自同构。

定理2.11 设 S 为一群，则 S 的所有自同构成为一个群，称为 S 的**自同构群**，记为 $\mathrm{Aut}(S)$。

证明 显然，幺映射 e 是一个自同构，故 $\mathrm{Aut}(S)$ 非空。设 σ 在 $\mathrm{Aut}(S)$ 中，因为 σ 为单满映射，所以其逆元素 σ^{-1} 存在并为一单满映射。我们只要证明 σ^{-1} 是群映射，即知 $\sigma^{-1} \in \mathrm{Aut}(S)$。令 s_1 及 s_2 为 S 中的任意二元素，s_3 及 s_4 适合下式

$$\sigma^{-1}(s_1) = s_3, \quad \sigma^{-1}(s_2) = s_4,$$

即

$$\sigma(s_3) = s_1, \quad \sigma(s_4) = s_2,$$

则有 $\sigma(s_3 * s_4) = \sigma(s_3) * \sigma(s_4) = s_1 * s_2$。故得

$$\sigma^{-1}(s_1 * s_2) = s_3 * s_4,$$

即

$$\sigma^{-1}(s_1 * s_2) = \sigma^{-1}(s_1) * \sigma^{-1}(s_2).$$

故知 $\sigma^{-1} \in \mathrm{Aut}(S)$。因为运算的合成是适合结合律的，而集合 $\mathrm{Aut}(S)$ 的双项运算就是映射的合成，所以有结合律。综上所述，知 $\mathrm{Aut}(S)$ 为一群。 ▎

讨论 不难看出，任何忠实地作用在群 S 上的变换群皆可理解成 $\mathrm{Aut}(S)$ 的一个子群。

例 15 $\mathrm{Aut}(\boldsymbol{Z}) = \{e, -e\}$。原因如下：整数群 $\boldsymbol{Z}$ 仅有两个不同的生成元集 $\{1\}$ 及 $\{-1\}$。设 $\sigma \in \mathrm{Aut}(\boldsymbol{Z})$，则 $\sigma(1) = 1$ 或 -1。如果 $\sigma(1) = 1$，则有

$$\sigma(n) = \sigma(1 + 1 + \cdots + 1) = \sigma(1) + \sigma(1) + \cdots + \sigma(1) = n,$$

即 σ 为幺映射 e。如果 $\sigma(1) = -1$，则有

$$\sigma(n) = \sigma(1 + 1 + \cdots + 1) = \sigma(1) + \sigma(1) + \cdots + \sigma(1) = -n,$$

即 $\sigma = -e$。

$\mathrm{Aut}(\boldsymbol{Z}_n)$ 与 $\boldsymbol{Z}_n^*$ 同构。原因如下：设 m 与 n 互素，则存在 $a, b \in \boldsymbol{Z}$，使得 $am + bn = 1$。对模 n 取剩余类，则得

$$a[m]_n = [1]_n,$$

这说明 $\boldsymbol{Z}_n^*$ 中每个元素皆是 $\boldsymbol{Z}_n$ 的生成元素。反之，设 $[l]_n$ 为 $\boldsymbol{Z}_n$ 的一个生成元素，则必有 $a \in \boldsymbol{Z}$，使得 $a[l]_n = [1]_n$。也即有 $b \in \boldsymbol{Z}$，使得 $al = 1 - bn$，即 l 与 n 互素，$[l]_n \in \boldsymbol{Z}_n^*$。显然，映射

$$\rho_{[m]}: [1]_n \to [m]_n$$

诱导出 $\boldsymbol{Z}_n$ 的一个自同构，而且

$$\rho_{[m]} \circ \rho_{[l]} = \rho_{[ml]}.$$

由此不难推出 $\mathrm{Aut}(\boldsymbol{Z}_n)$ 与 $\boldsymbol{Z}_n^*$ 同构。

例16 取 $\boldsymbol{Z} \oplus \boldsymbol{Z} = \{(a, b): a, b \in \boldsymbol{Z}\}$。其中加法的定义如下：

$$(a, b) + (c, d) = (a + c, b + d).$$

不难看出，在这种加法的定义下，$\boldsymbol{Z} \oplus \boldsymbol{Z}$ 成为一群，此群或记为 $\boldsymbol{Z}^2$。同样的方法，令 $G_1, G_2, \cdots, G_n$ 皆为群，可定义一个新的群

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_n$$
$$= \{(a_1, a_2, \cdots, a_n): a_i \in G_i,\ i = 1, 2, \cdots, n\},$$

其双项运算定义为

$$(a_1, a_2, \cdots, a_n) * (b_1, b_2, \cdots, b_n)$$
$$= (a_1 * b_1, a_2 * b_2, \cdots, a_n * b_n).$$

这样定义的群 G，称为 $G_1, G_2, \cdots, G_n$ 的直积。如果 $G_1 = G_2 = \cdots = G_n$，则 G 也可以写成 G_1^n。

$\boldsymbol{Z}^2$ 可以理解成平面上的网格点的集合，有广泛的应用价值。设 $\sigma \in \mathrm{Aut}(\boldsymbol{Z}^2)$。把 (a_1, a_2) 写成列向量

$$\begin{bmatrix} a_1 \\ a_2 \end{bmatrix}.$$

设

$$\sigma\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) = \begin{bmatrix} b_{11} \\ b_{21} \end{bmatrix}, \quad \sigma\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right) = \begin{bmatrix} b_{12} \\ b_{22} \end{bmatrix}.$$

不难看出

$$\sigma\left(\begin{bmatrix} a_1 \\ a_2 \end{bmatrix}\right) = \sigma\left(a_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + a_2 \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right)$$

$$= \begin{bmatrix} a_1 b_{11} + a_2 b_{12} \\ a_1 b_{21} + a_2 b_{22} \end{bmatrix} = C_\sigma \begin{bmatrix} a_1 \\ a_2 \end{bmatrix},$$

其中
$$C_\sigma = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}.$$

不难看出

$$\rho \circ \sigma\left(\begin{bmatrix} a_1 \\ a_2 \end{bmatrix}\right) = C_{\rho \circ \sigma} \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} = C_\rho C_\sigma \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}.$$

如果取 $\rho = \sigma^{-1}$，则有 $C_{\sigma^{-1}} C_\sigma = I_2$，其中 I_2 为二阶幺矩阵。上式两端取行列式，得出

$$(\det C_{\sigma^{-1}})(\det C_\sigma) = 1.$$

而此式左端的行列式皆为整数，故只能等于1或 -1。这种行列式为 ± 1 的二阶整数矩阵构成一群，称为二阶的**特殊整数线性群**，记为 $SL(2,\boldsymbol{Z})$。从上面讨论可以看出，$\mathrm{Aut}(\boldsymbol{Z}^2)$ 即是 $SL(2,\boldsymbol{Z})$。同法可以得知 $\mathrm{Aut}(\boldsymbol{Z}^n)$ 即是 n 阶的特殊整数线性群 $SL(n,\boldsymbol{Z})$。▌

上节的定理2.6的系，证明了一群 G 的心是 G 的正规子群。而群的心即是使内自同构 τ_g 为幺映射的元素 g 的集合。根据定理2.10，群 G 对其心作商群以后，则忠实地以内自同构作用于群 G。这一商群称为群 G 的**内自同构群**，记为 $\mathrm{Inn}(G)$。

在例14及例15中，群 $\boldsymbol{Z},\boldsymbol{Z}_n$ 以及 $\boldsymbol{Z}^n$ 皆是交换群，故其内自同构群都是幺群，因此是自同构群的正规子群。一般言之，我们有如下的定理。

定理2.12 一群 G 的内自同构群 $\mathrm{Inn}(G)$ 是自同构群 $\mathrm{Aut}(G)$ 的正规子群。

证明 设 g_1,g_2 为 G 的任意二元素，τ_{g_1} 为 g_1 引生的内自同构，σ 为 $\mathrm{Aut}(G)$ 的任意元素。则有

$$\begin{aligned}\sigma\circ\tau_{g_1}\circ\sigma^{-1}(g_2)&=\sigma(g_1*\sigma^{-1}(g_2)*g_1^{-1})\\&=\sigma(g_1)*\sigma(\sigma^{-1}(g_2))*\sigma(g_1)^{-1}\\&=\sigma(g_1)*g_2*\sigma(g_1)^{-1}=\tau_{\sigma(g_1)}(g_2).\end{aligned}$$

故 $\sigma\circ\tau_{g_1}\circ\sigma^{-1}\in\mathrm{Inn}(G)$。所以 $\mathrm{Inn}(G)$ 是 $\mathrm{Aut}(G)$ 的正规子群。▌

习 题

1. 令 $G=\boldsymbol{Z}/6\boldsymbol{Z}$，证明 $\mathrm{Aut}(G)\neq\mathrm{Inn}(G)$。
2. 证明 $\mathrm{Aut}(S_3)=\mathrm{Inn}(S_3)\approx S_3$。
3. 试确定 $\mathrm{Aut}(\boldsymbol{Q})$。
4. 试找出复整数加群的自同构群。
5. 设 $G=G_1\oplus G_2\oplus\cdots\oplus G_n$，其中 G_i 为 $p_i^{r_i}$ 阶循环群(p_i 均为素数，且 $p_i\neq p_j(i\neq j)$)。求 $o(\mathrm{Aut}(G))$。
6. 找出 $\mathrm{Aut}(\boldsymbol{Z}/n\boldsymbol{Z}\oplus\boldsymbol{Z}/m\boldsymbol{Z})$，其中 $(m,n)=(1)$。

7. 设 G 的阶是25，G 不是循环群。确定 $\mathrm{Aut}(G)$。

8. 设 G 为 r 个 p 阶循环群的直积，证明

$$o(\mathrm{Aut}(G))=(p^r-1)(p^r-p)\cdots(p^r-p^{r-1}).$$

9. 令 G 为四元数群(参考§1习题7)。试确定 $\mathrm{Aut}(G)$。

10. 设 α 为群 G 的自同构，C 为 G 的心。如果

$$x^{-1}\alpha(x)\in C\quad(\forall x\in G),$$

则称 α 为 G 的**中心自同构**。证明

(1) G 的所有中心自同构成群；

(2) 中心自同构群含于内自同构群；

(3) 中心自同构群与 G/C 的中心同构。

§6 p 群及西洛定理

在本节内，我们将研究有限群的内部是否含有某些阶数的子群以及其可能有多少个。

令一群 G 以内自同构作用于群 G 上，则群 G 被划分成一些分离的共轭类，即轨道。于是我们得到下述的**共轭类方程式**

$$o(G)=\sum(\text{共轭类的基数}).$$

定理2.13 设群 G 为一个"p 群"，即基数 $o(G)$ 为 p^n 的群，此处 p 为一个确定的素数，n 为正整数。则 G 的心不是幺群。

证明 设 C 为 G 的任一共轭类，$g\in C$。由定理2.5，有

$$C\text{ 的基数}=[G:\mathrm{Stab}(g)].$$

故 C 的基数是 $o(G)$ 的因数。而 $o(G)=p^n$，故得

$$C\text{ 的基数}=p^m,\qquad 0\leqslant m\leqslant n.$$

G 的幺元构成的子集 $\{e\}$ 显然是一个共轭类，即存在一个共轭类的基数为1．现注意共轭类方程式的两边，其左边被 p 整除，右边为形如 p^m 的数之和，而这些数中已经有一个数为1，故右边至少还应出现 $p-1$ 个1。任取其中一个1，它所对应的共轭类是幺集 $\{g\}$。显然，$g\neq e$，并且 g 在群 G 的心中。▌

定理2.14 设群 G 为一 p 群，$o(G)=p^n$。则存在一系列的子群 $G_i(i=0,1,\cdots,n)$，其中 G_i 是 G_{i+1} 的正规子群，即

$$G=G_n\triangleright G_{n-1}\triangleright\cdots\triangleright G_{i+1}\triangleright G_i\triangleright\cdots\triangleright G_0=\{e\},$$

而且每个商群 G_{i+1}/G_i 都是 p 阶循环群。

证明 令 C 为 G 的心，根据上面的定理知 C 不是幺群。设 g 为 C 中一个非幺元素，C_1 为 g 生成的子群。由于

$$o(C_1)\mid o(G),$$

故 C_1 的阶数必形如 $p^m(m\geqslant 1)$。令 $G_1=\langle g^{p^{m-1}}\rangle$。不难看出，$G_1$ 是 G 的 p 阶正规子群。

下面我们用归纳法。如果 $o(G)=p^1$，则取 $G_1=G$ 即可。设此定理对阶数为 p^{n-1} 的群皆成立，按照上面的讨论，知有一 p 阶正规子群 G_1。令 $G^*=G/G_1$，则 $o(G^*)=p^{n-1}$。依照归纳法假设，在 G^* 中存在一系列子群 G_i^*，如下图：

$$\begin{array}{l} G \\ \downarrow{\scriptstyle \kappa} \\ G/G_1=G^*=G^*_{n-1}\triangleright G^*_{n-2}\triangleright\cdots G^*_i\triangleright\cdots\triangleright G^*_0=\{e\}\end{array}$$

其中 κ 是 G 到商群 G/G_1 的典型映射。取 G_i^* 在 κ 下的象源，记为 G_{i+1}。根据定理2.7，我们知道 G_i 皆是 G_{i+1} 的正规子群。于是得出

$$G=G_n\triangleright G_{n-1}\triangleright\cdots\triangleright G_{i+1}\triangleright\cdots\triangleright G_1\triangleright G_0=\{e\}.$$

显然，G_{i+1}/G_i 皆为 p 阶循环群。▌

讨论 1）此定理中的一系列子群称为“合成群列”，其详情见下节。

2）在“域论”中本定理有应用价值，详情见第五章。

3）显然有 $o(G_i)=p^i(i=0,1,\cdots,n)$。

4）同法可以证明，如果 $o(G)=p^n$，则存在一系列的正规子群 G_i，使得

$$G=G_n\supsetneqq G_{n-1}\supsetneqq\cdots\supsetneqq G_i\supsetneqq\cdots\supsetneqq G_0=\{e\}.$$

这种群即所谓的**幂零群**。详情请参考群论的专著。 ∎

以下我们将证明三个"西洛定理"。

定理2.15(第一西洛定理) 设群 G 的阶数为 $o(G)=mp^n$。其中 p 为素数，$p\nmid m$。则 G 有一个阶数为 p^n 的子群 H。

证明 令 S 为 G 中基数为 p^n 的子集的集合，即

$$S=\{s:\ s\subset G,\ s\text{ 的基数为 }p^n\}。$$

令群 G 从左侧作用在 S 上，即

$$g(s)=\{g*g':\ g'\in s\}。$$

则 G 是集合 S 上的变换群。

$$S\text{的基数}=\binom{mp^n}{p^n}$$

$$=\frac{mp^n(mp^n-1)\cdots(mp^n-i)\cdots(mp^n-p^n+1)}{p^n(p^n-1)\cdots(p^n-i)\cdots1}。$$

在上式的右端，考虑

$$\frac{mp^n-i}{p^n-i}。$$

不难看出，此分数的分母及分子中的 p 的因子恰好抵消，于是得知 S 的基数不被 p 整除。又有

$$S\text{ 的基数}=\sum(\text{轨道的基数})，$$

于是必有一轨道的基数不被 p 整除。记此轨道为 C。设 s 为 C 中一元素，令 $H=\mathrm{Stab}(s)$，我们将证 $o(H)=p^n$。根据定理2.5，有

$$C\text{ 的基数}=[G:\mathrm{Stab}(s)]=[G:H]，$$

又有
$$o(G)=[G:H]\cdot o(H)。$$

由上面二式知 $p^n|o(H)$，于是有 $o(H)\geqslant p^n$。又对 s 中任一元素 g 而言，有 $H(g)=\{h*g:\ h\in H\}\subset s$。故

$$o(H)=H(g)\text{的基数}\leqslant s\text{ 的基数}=p^n。$$

于是 $o(H)=p^n$。 ∎

讨论 此定理证明了 $mp^n(p\nmid m)$阶群必有 p^n 阶子群。凡是

这种 p^n 阶子群，皆称为**西洛 p 子群**。

定理2.16（第二西洛定理） 设 G 为有限群。则在内自同构作用下，G 的所有西洛 p 子群皆属于同一轨道。换言之，西洛 p 子群皆共轭。

证明 设 $o(G)=mp^n$，其中 $p\nmid m$。设 H 为一个西洛 p 子群。令 $S=\{g_1*H, g_2*H, \cdots, g_m*H\}$ 为 G 对 H的陪集之集合。其中有一个陪集是 H，不妨假设 $g_1*H=H$。如令 G 自左侧作用在 S 上，不难看出，此时只有一条轨道，即 S 自身。由此即知

$$[G:\mathrm{Stab}(g_i*H)]=S\text{ 的基数}=m,\quad \forall i=1,2,\cdots,m.$$

所以 $o(\mathrm{Stab}(g_i*H))=p^n$。又由

$$(g_i*H*g_i^{-1})*(g_i*H)=g_i*H,$$

知
$$g_i*H*g_i^{-1}\subset \mathrm{Stab}(g_i*H),$$

而 $g_i*H*g_i^{-1}$ 的基数也是 p^n，故有

$$g_i*H*g_i^{-1}=\mathrm{Stab}(g_i*H),\quad \forall i=1,2,\cdots,m.$$

现在我们任取一西洛 p 子群 H'，只考虑子群 H' 在S 上的作用，则在此缩小了的作用之下，S 又被重新划分成一些轨道。于是有

$$m=S\text{ 的基数}=\sum(\text{轨道的基数}).$$

因为 m 不被 p 整除，故必有某轨道的基数不被 p 整除。记此轨道为 C。设 g_i*H 为 C 中一元素，则有

$$C\text{ 的基数}=[H':(\text{在 }H'\text{作用下 }g_i*H\text{ 的稳定群})].$$

故 C 的基数又必是 p 的方幂，所以 C 的基数必为 1。这意味着

$$H'\subset \mathrm{Stab}(g_i*H)$$

（这里的 $\mathrm{Stab}(g_i*H)$是在 G 作用下 g_i*H 的稳定群）。而两者的基数相同，故

$$H'=\mathrm{Stab}(g_i*H).$$

结合前面证出的结果，即有

$$H'=g_i*H*g_i^{-1}.\quad \blacksquare$$

定理2.17（第三西洛定理） 设 $o(G)=mp^n$，其中 p 为素数，

$p \nmid m$。令 r 为西洛 p 子群的个数，则有

1) $r|m$；

2) $r \equiv 1 (\bmod p)$。

证明 1) 令 H 为一个西洛 p 子群。设在 G 以内自同构作用下 H 的轨道为 T，即

$$T = \{g_i * H * g_i^{-1}: g_i \in G\}.$$

根据第二西洛定理，T 的基数即为 r。按照定理2.5，

$$r = [G:\mathrm{Stab}(H)].$$

又显然有 $H \subset \mathrm{Stab}(H)$，故有 $r|[G:H] = m$。

2) 如第二西洛定理的证明，令 H 为一西洛 p 子群，

$$S = \{g_1 * H, g_2 * H, \cdots, g_m * H\}.$$

令 G 自左侧作用在 S 上。在第二西洛定理的证明中已有

$$\mathrm{Stab}(g_i * H) = g_i * H * g_i^{-1}.$$

如果 $g_i * H * g_i^{-1}$ 是 $g_j * H$ 的稳定群，则

$$g_i * H * g_i^{-1} * g_j * H = g_j * H,$$

即
$$H * (g_i^{-1} * g_j * H) = g_i^{-1} * g_j * H.$$

亦即 H 是 $g_i^{-1} * g_j * H$ 的稳定群。反之也对。于是，如果 H 是 S 中 k 个元素 $g_l * H$（l 取$1, 2, \cdots, m$ 中 k 个数）的稳定群，则 $g_i * H * g_i^{-1}$ 也是 S 中 k 个元素 $g_i * g_l * H$ 的稳定群。按照稳定群的异同将 S 的元素分类，则共有 r 类，每类中有 k 个元素，故

$$m = rk.$$

再考虑 H 自左侧作用在 S 上。在这种缩小了的作用下，S 被分成许多轨道。自然有

$$m = S\text{ 的基数} = \sum(\text{轨道的基数}).$$

而且根据定理2.5，有

$$g_l * H\text{ 所在轨道的基数} = [H : g_l * H\text{ 在 }H\text{ 中的稳定群}]$$
$$= p^q \quad (0 \leqslant q \leqslant n).$$

注意到这些轨道中有 k 个是幺集，故有

$$rk = m = k + ap \equiv k (\bmod p).$$

因$p\nmid m$，故$p\nmid k$，从上式两端消去k，即有

$$r\equiv 1(\bmod p). \quad \blacksquare$$

习　题

1. 设G为有限群，P为G的一个西洛p子群，$N\lhd G$。证明PN/N是G/N的西洛p子群。

2. 设G为有限群，P为G的一个西洛p子群，证明

(1) P在$N(P)$中的共轭子集只有一个；

(2) $N(P)=N(N(P))$，

其中$N(P)$表示P的正规化子(见§3习题4)。

3. 设G是有限群，$H<G$。证明H的西洛p子群必然形如$L\cap H$，此处L是G的一个西洛p子群。

4. 证明阶为15,35,77的群必然是循环群。

5. 设p,q为两个素数，$p<q$，且$q\not\equiv 1(\bmod p)$。证明阶为pq的群必是循环群。

6. 设p为素数。证明阶为p^2的群必是交换群。

7. 设G的阶为100，证明G中必有一个阶为25的正规子群。

8. 设G的阶为168，G中有多少个阶为7的元素?

9. 设p为素数。证明$2p$阶群或是循环群，或与正p边形的对称群(即所谓"二面体群"(dihedral group))D_p同构。

10. 设n是奇数。证明阶为$2n$的群必含有n阶子群。

11. 找出S_3,S_4,S_5的所有西洛2子群及西洛3子群。

12. 写出所有互不同构的8阶群。

13. 证明30阶群必非单群(单群即不含有非平凡的正规子群的群)。

14. 设p,q为素数。证明p^2q阶群必非单群。

15. 证明阶数小于60的单群的阶必为素数。

§7 若当-荷德定理

在上节的定理2.14中，我们证明在p群中有一系列的子群

$$G=G_n\rhd G_{n-1}\rhd\cdots\rhd G_0=\{e\}.$$

这一系列子群有很重要的意义。就群论本身而言，这些子群将提示我们构造群G的方法；就群论的应用而言，这些子群将帮助我们利用G_i来逐步简化某些现象。关于前者，请读者参考群论的专著；关于后者，请参看本书第五章"域论"中的伽罗瓦理论。

定义2.18 设G为一群。G中的一系列子群

$$G=G_n\rhd G_{n-1}\rhd\cdots\rhd G_i\rhd\cdots\rhd G_0=\{e\}$$

(其中G_i为G_{i+1}的正规子群，且不等于G_{i+1})称为G的**正规群列**。集合

$$\{G_{i+1}/G_i;\ i=0,1,\cdots,n-1\}$$

称为这个正规群列的**商群集**。如果另有一个正规群列

$$G=G_m^*\rhd G_{m-1}^*\rhd\cdots\rhd G_0^*=\{e\}$$

具有如下的性质：每一个G_i皆在第二个正规群列中出现，则称第二个正规群列是第一个正规群列的**细化**。如果一个正规群列除其本身之外再无其它的细化，则称为**合成群列**。

例16 在上节定理2.14中的p群的正规群列

$$G=G_n\rhd G_{n-1}\rhd\cdots\rhd G_0=\{e\}$$

(其中$o(G_{i+1}/G_i)=p$, $\forall i=0,1,\cdots,n-1$) 是一个合成群列。其理由如下：

设在G_{i+1}与G_i之间能插入一个G_{i+1}的正规子群H。考虑G_{i+1}到G_{i+1}/G_i的典型映射κ，则$\kappa(H)$必为G_{i+1}/G_i的子群。而$o(G_{i+1}/G_i)$为素数p，所以$o(\kappa(H))$为1或p，也即$\kappa(H)$为幺群或整个群G_{i+1}/G_i。由此得出H为G_i或G_{i+1}。故G_{i+1}与G_i之间不能插入G_{i+1}的任何异于G_i和G_{i+1}的正规子群。

取如此构造出来的两个合成群列，则其商群集皆是 n 个阶数为 p 的群的集合。于是这两个商群集从抽象的观点来说是完全一样的。对一般的群，同样的结论也是成立的。这就是以下的定理2.20(通称为若当-荷德定理)。

另外，我们考虑 $G=\boldsymbol{Z}/6\boldsymbol{Z}$ 的加法群. G 有两个非平凡的子群

$$G_2=2\boldsymbol{Z}/6\boldsymbol{Z},\quad G_3=3\boldsymbol{Z}/6\boldsymbol{Z}.$$

不难看出，G 有下列三个正规群列

$$G\rhd\{e\},\quad G\rhd G_2\rhd\{e\},\quad G\rhd G_3\rhd\{e\}.$$

而且后两个是合成群列。其商群集分别是

$$\{G/G_2\ ,G_2/\{e\}\},\qquad \{G/G_3\ ,G_3/\{e\}\},$$

亦即

$$\{\boldsymbol{Z}/2\boldsymbol{Z},2\boldsymbol{Z}/6\boldsymbol{Z}\},\qquad \{\boldsymbol{Z}/3\boldsymbol{Z},3\boldsymbol{Z}/6\boldsymbol{Z}\}.$$

不难看出 $\boldsymbol{Z}/2\boldsymbol{Z}$ 与 $3\boldsymbol{Z}/6\boldsymbol{Z}$ 同构，$2\boldsymbol{Z}/6\boldsymbol{Z}$ 与 $\boldsymbol{Z}/3\boldsymbol{Z}$ 同构。也即这两个商群集之间有一个单满映射，使相对应的商群互为同构. ▌

在讨论若当-荷德定理之前，我们先证明群映射的第二同构定理及第三同构定理。第一同构定理即 § 4 中的定理2.9.

定理2.18(第二同构定理) 设 H 为群 G 的子群，N 为 G 的正规子群。则

1) $H\cap N$ 为 H 的正规子群；

2) $H*N=\{h*n:\ h\in H,n\in N\}$ 为 G 的子群；

3) N 为 $H*N$ 的正规子群. 令 ρ 为由 $H*N/N$ 到 $H/H\cap N$ 的自然映射，其定义如下：

$$\rho(h*n*N)=h*(H\cap N),$$

则 ρ 为同构。

证明 1) $e\in H\cap N$，故 $H\cap N$ 非空。设有 $a,b\in H\cap N$，则有

$$a*b^{-1}\in H,\qquad a*b^{-1}\in N,$$

故 $a*b^{-1}\in H\cap N$，即知 $a*b^{-1}$ 为一子群。令 H 以内自同构作用于 G 上，则 N 及 H 皆为不变子集，故两者的交集 $H\cap N$ 也为不变子集。于是 $H\cap N$ 为 H 的正规子群。

2) $e\in H*N$，故 $H*N$ 非空。设 $a,b\in H*N$，即有 $h_1,h_2\in H$，$n_1,n_2\in N$，使得

$$a=h_1*n_1,\qquad b=h_2*n_2.$$

于是

$$\begin{aligned}a*b^{-1}&=(h_1*n_1)*(h_2*n_2)^{-1}\\&=h_1*h_2^{-1}*(h_2*n_1*n_2^{-1}*h_2^{-1}),\end{aligned}$$

而 N 为 G 的正规子群，故上式右端括号中的元素在 N 中，即 $a*b^{-1}$ 在 $H*N$ 中，所以 $H*N$ 为一子群。

3) N 自然是 $H*N$ 的子群。N 为 G 的正规子群，即在 G 的内自同构作用下 N 为不变子集，自然在 $H*N$ 的内自同构作用下也是不变子集，所以 N 是 $H*N$ 的正规子群。

以上是证明 ρ 为同构的准备工作。下面我们首先要证明 ρ 的定义是有意义的。设

$$h_1*n_1*N=h_2*n_2*N,$$

即 $h_1*N=h_2*N$，也即 $h_1^{-1}*h_2\in N$。显然 $h_1^{-1}*h_2\in H$，故有

$$h_1^{-1}*h_2\in H\cap N,$$

即

$$h_1*(H\cap N)=h_2*(H\cap N).$$

这就说明了 ρ 的定义是有意义的。

易于证出 ρ 是群映射。事实上

$$\begin{aligned}&\rho((h_1*n_1*N)*(h_2*n_2*N))\\&=\rho((h_1*N)*(h_2*N))\\&=\rho(h_1*h_2*N)=h_1*h_2*(H\cap N)\\&=h_1*(H\cap N)*h_2*(H\cap N)\\&=\rho(h_1*n_1*N)*\rho(h_2*n_2*N).\end{aligned}$$

我们再证 ρ 是一单射。设 $\rho(h_1*n_1*N)=\rho(h_2*n_2*N)$，则有

$$h_1*(H\cap N)=h_2*(H\cap N),$$

即

$$h_1^{-1}*h_2\in H\cap N\subset N,\qquad h_1*N=h_2*N,$$

即有 $$h_1 * n_1 * N = h_2 * n_2 * N.$$

最后我们证明 ρ 是一满射。事实上，设 $h*(H\cap N)$ 是 H 对 $H\cap N$ 的任一陪集，则 $h*e*N$ 即是它的一个象源。

综上可知 ρ 为一同构。 ▌

定理2.19（第三同构定理） 设 H_1 及 H_2 为群 G 的子群，N_1 为 H_1 的正规子群，N_2 为 H_2 的正规子群。则

1) $N_1*(H_1\cap N_2)$ 为 $N_1*(H_1\cap H_2)$ 的正规子群，$N_2*(H_2\cap N_1)$ 为 $N_2*(H_2\cap H_1)$ 的正规子群；

2) $(H_1\cap N_2)*(H_2\cap N_1)$ 是 $H_1\cap H_2$ 的正规子群；

3) 以上的三个商群

$$N_1*(H_1\cap H_2)/N_1*(H_1\cap N_2),$$

$$N_2*(H_2\cap H_1)/N_2*(H_2\cap N_1)$$

及 $$H_1\cap H_2/(H_1\cap N_2)*(H_2\cap N_1)$$

皆同构。

证明 1) 由于 $H_1\cap N_2$ 及 $H_1\cap H_2$ 皆是 H_1 的子群，而 N_1 是 H 的正规子群，由前一定理，知 $N_1*(H_1\cap N_2)$ 及 $N_1*(H_1\cap H_2)$ 皆为 H_1 的子群。令

$$a=n_1*h\in N_1*(H_1\cap H_2),$$

τ_a 为 a 引生的内自同构。注意到 $H_1\cap N_2$ 是 $H_1\cap H_2$ 的正规子群，即知

$$\begin{aligned}
&\tau_a(N_1*(H_1\cap N_2))\\
&\quad=n_1*h*N_1*(H_1\cap N_2)*h^{-1}*n_1^{-1}\\
&\quad=n_1*N_1*h*(H_1\cap N_2)*h^{-1}*n_1^{-1}\\
&\quad=N_1*(H_1\cap N_2)*h*h^{-1}*n_1^{-1}\\
&\quad=N_1*(H_1\cap N_2)*n_1^{-1}.
\end{aligned}$$

对于 $H_1\cap N_2$ 中的任意元素 m，总有一相应的 $n_3\in N_1$，使得

$$m*n_1^{-1}=n_3*m$$

（这因为 N_1 是 H_1 的正规子群，而 $m\in H_1$），故

$$N_1 * (H_1 \cap N_2) * n_1^{-1}$$
$$= \{n_1 * m * n_1^{-1}:\ n \in N_1,\ m \in H_1 \cap N_2\}$$
$$= \{n_1 * n_3 * m:\ n \in N_1,\ m \in H_1 \cap N_2\}$$
$$= \{n_1 * m:\ n \in N_1,\ m \in H_1 \cap N_2\} = N_1 * (H_1 \cap N_2).$$

所以$N_1 * (H_1 \cap N_2)$是$N_1 * (H_1 \cap H_2)$的正规子群. 同样可证$N_2 * (H_2 \cap N_1)$是$N_2 * (H_2 \cap H_1)$的正规子群.

2) 由$H_1 \cap N_2$及$H_2 \cap N_1$皆为$H_1 \cap H_2$的正规子群，不难导出$(H_1 \cap N_2) * (H_2 \cap N_1)$是$H_1 \cap H_2$的正规子群.

3) 我们定义一个由

$$N_1 * (H_1 \cap H_2) \text{ 到 } H_1 \cap H_2 / (H_1 \cap N_2) * (H_2 \cap N_1)$$

的映射 ρ. 对于 $n_1 \in N_1$, $h \in H_1 \cap H_2$, 令

$$\rho(n_1 * h) = h * (H_1 \cap N_2) * (H_2 \cap N_1).$$

首先，我们要证明ρ的定义是有意义的. 设$n_1' * h' = n_1 * h$, 则

$$h_1' * h^{-1} = (n_1')^{-1} * n_1 \in N_1 \cap (H_1 \cap H_2)$$
$$= N_1 \cap H_2 \subset (H_1 \cap N_2) * (H_2 \cap N_1),$$

即 h_1' 与 h 属于$(H_1 \cap N_2) * (H_2 \cap N_1)$的同一个陪集，故有

$$\rho(n_1' * h') = \rho(n_1 * h),$$

故 ρ 的定义是有意义的.

其次，我们要证明 ρ 是一个群映射. 设又有

$$\bar{n}_1 \in N_1, \quad \bar{h} \in H_1 \cap H_2,$$

则有

$$\rho(n_1 * h * \bar{n}_1 * \bar{h}) = \rho(n_1 * \tilde{n}_1 * h * \bar{h})$$
$$= h * \bar{h} * (H_1 \cap N_2) * (H_2 \cap N_1)$$
$$= h * (H_1 \cap N_2) * (H_2 \cap N_1) * \bar{h}(H_1 \cap N_2) * (H_2 \cap N_1)$$
$$= \rho(n_1 * h) * \rho(\bar{n}_1 * \bar{h}),$$

其中$\tilde{n}_1$是N_1中的元素，满足$h * \bar{n}_1 = \tilde{n}_1 * h$. 故 ρ 为群映射.

我们再证明ρ的核为$N_1 * (H_1 \cap N_2)$. 容易看出

$$\ker(\rho) \supset N_1 * (H_1 \cap N_2).$$

反之，设$n_1 * h \in \ker\rho$，即

$$\rho(n_1 * h) = h * (H_1 \cap N_2) * (H_2 \cap N_1)$$
$$= (H_1 \cap N_2) * (H_2 \cap N_1),$$

也即$h \in (H_1 \cap N_2) * (H_2 \cap N_1)$。于是

$$h = h_1 * h_2,$$

其中$h_1 \in H_1 \cap N_2$，$h_2 \in H_2 \cap N_1 \subset N_1$。故

$$h \in (H_1 \cap N_2) * N_1 = N_1 * (H_1 \cap N_2).$$

显然ρ是满射。根据第一同构定理(定理2.9)的系，我们得知商群

$$N_1 * (H_1 \cap H_2)/N_1 * (H_1 \cap N_2) \text{ 与 }$$
$$H_1 \cap H_2/(H_1 \cap N_2) * (H_2 \cap N_1)$$

同构。同法可证

$$N_2 * (H_2 \cap H_1)/N_2 * (H_2 \cap N_1) \text{ 与 }$$
$$H_1 \cap I' \quad (H_1 \cap N_2) * (H_2 \cap N_1)$$

同构。▌

现在我们回到若当-荷德定理的本文。

定理2.20(若当-荷德定理) 设群G有一合成群列，则G的任意两个合成群列的商群集之间有一个单满映射，使相对应的商群为同构的。

讨论 如果G为有限群，则G显然有合成群列。如果每一个正规群列皆可细化成合成群列，则本定理等同于下面的定理。在一般情形下，本定理皆可由下面的定理导出。因此我们先证明下面的定理，再回过头来讨论定理2.20。

定理2.21(许来尔定理) 群G的任意两个正规群列皆可以细化，使细化后的两个正规群列的商群集之间有一个单满映射，而相对应的商群为同构的。

证明 设此两个正规群列为

$$G = G_n \rhd G_{n-1} \rhd \cdots \rhd G_i \rhd \cdots \rhd G_0 = \{e\},$$
$$G = G'_m \rhd G'_{m-1} \rhd \cdots \rhd G'_j \rhd \cdots \rhd G'_0 = \{e\}.$$

令

$$G_{ij}=G_{i-1}*(G_i\cap G'_j),\quad G'_{ji}=G'_{j-1}*(G'_j\cap G_i)$$
$$(i=1,2,\cdots,n,\quad j=1,2,\cdots,m).$$

则可以排成下列两个矩阵：

$$\begin{bmatrix} G_{nm} & G_{n,m-1} & \cdots & G_{n0} \\ G_{n-1,m} & G_{n-1,m-1} & \cdots & G_{n-1,0} \\ \cdots & \cdots & \cdots & \cdots \\ G_{0m} & G_{0,m-1} & \cdots & G_{00} \end{bmatrix}$$

及

$$\begin{bmatrix} G'_{mn} & G'_{m,n-1} & \cdots & G'_{m0} \\ G'_{m-1,n} & G'_{m-1,n-1} & \cdots & G'_{m-1,0} \\ \cdots & \cdots & \cdots & \cdots \\ G'_{0n} & G'_{0,n-1} & \cdots & G'_{00} \end{bmatrix}.$$

请注意每个矩阵的第一列与最后一列的关系：

$$G_{im}=G_{i-1}*(G_i\cap G'_m)=G_{i-1}*(G_i\cap G)$$
$$=G_{i-1}*G_i=G_i=G_i*(G_{i+1}\cap G'_0)=G_{i+1,0}$$

及

$$G'_{in}=G'_{i+1,0}.$$

按照第三同构定理(定理2.19)，上面两个矩阵的每一行中后面的子群是前一个子群的正规子群，即

$$G_{ij}\rhd G_{i,j-1},\quad G'_{ji}\rhd G'_{j,i-1},$$

并且二商群

$$G_{ij}/G_{i,j-1}\quad 与\quad G'_{ji}/G'_{j,i-1}$$

同构。如果我们把这两个矩阵都一行一行地排成一长列，并且把相同子群抛去(即把商群集中的幺群抛去)，则分别得出原来的两个正规群列的细化。而上面已给出了两个商群集之间的一个单满映射，使相应的商群同构。▌

讨论 1) 我们用许来尔定理(定理2.21)推导若当-荷德定理(定理2.20)：设群G有两个合成群列，则此二合成群列皆是正规群列，而且除本身外再无进一步的细化。于是按照许来尔定理，

此二合成群列的商群集之间有一单满映射，使相应的商群为同构的。

2）一般言之，一个群G并不一定有合成群列。例如取$\boldsymbol{Z}$中的任意的正规群列

$$\boldsymbol{Z}=G_n \triangleright G_{n-1} \triangleright \cdots \triangleright G_1 \triangleright G_0=\{0\},$$

则在G_1与G_0之间总可以插入$2G_1$。

定义2.19 如果群G除了幺群及G本身之外，没有其它的正规子群，则称G为**单群**。

引理1 群G的一正规群列是合成群列的充要条件，是其商群集为单群的集合。

证明 设此正规群列为

$$G=G_n \triangleright G_{n-1} \triangleright \cdots \triangleright G_i \triangleright \cdots \triangleright G_0=\{e\}.$$

由第一同构定理，G_{i+1}与G_i之间不能插入另一正规子群的充要条件是G_{i+1}/G_i除了幺群及其本身外无其它的正规子群，即G_{i+1}/G_i为单群。▎

引理2 如果群G有一合成群列，则G的任意正规群列皆可细化成合成群列。

证明 根据定理2.21，此一正规群列可以细化成一个新的正规群列，使其商群集与已给的合成群列的商群集之间有一个对应关系。于是此二商群集都是单群的集合，根据上面的引理1，此一新的正规群列是合成群列。▎

定义2.20 如果一个群G有合成群列，则群G的**长度**定义为其合成群列中子群的个数减1，即其商群集的基数，记为$l(G)$。

定义2.21 如果群G有一个正规群列，其商群集为交换群集，则此群称为**可解群**。

关于可解群，我们有下面的定理。

定理2.22 设H是群G的正规子群，则G是可解群$\Longleftrightarrow H$及G/H都是可解群。

证明 $\Longrightarrow$。应用定理2.21，正规群列$G \triangleright H \triangleright \{e\}$可以细化

成

$$G=G_n\triangleright G_{n-1}\triangleright\cdots\triangleright G_i=H\triangleright\cdots\triangleright\{e\},$$

使其商群皆为交换群。根据第一同构定理，有

(1) $(G_j/H)/(G_{j-1}/H)\approx G_j/G_{j-1}$, $j=n,n-1,\cdots,i+1$.

故以下二正规群列

(2) $$H=G_i\triangleright G_{i-1}\triangleright\cdots\triangleright\{e\},$$

(3) $$G/H=G_n/H\triangleright G_{n-1}/H\triangleright\cdots\triangleright G_i/H=\{\bar{e}\}$$

的商群皆为交换群，即H与G/H均为可解群。

$\Longleftarrow$。若已给定正规群列(2)及(3)，其商群皆为交换群，则立即得到G的正规群列

$$G=G_n\triangleright G_{n-1}\triangleright\cdots\triangleright G_i=H\triangleright G_{i-1}\triangleright\cdots\triangleright\{e\},$$

根据(1)式，知此正规群列的商群皆为交换群，即G为可解群。 ▌

习　题

1. 利用若当-荷德定理讨论$\mathbf{Z}/n\mathbf{Z}$的合成群列，并由此导出算术基本定理，即整数分解成素数乘积的存在性和唯一性。

2. 设群G有一正规循环子群H，且G/H是循环群，那么G是否必然是循环群？

3. 找出二面体群D_4的所有合成群列(参考§6习题9)。

4. 找出S_3,S_4的所有合成群列。

5. 找出三维实空间的所有有限旋转群的合成群列。

6. 设p,q为素数。证明p^2q阶群必为可解群。

7. 设G为825阶群，证明G为可解群。

8. 证明可解群的任一子群皆为可解群。

9. 证明G为可解群$\Longleftrightarrow$ G的合成群列

$$G=G_n\triangleright G_{n-1}\triangleright\cdots\triangleright G_0=\{e\}$$

具有性质：G_i/G_{i-1}为素数阶循环群($\forall i=1,2,\cdots,n$)。

10. 参考§3习题9。令

$$G''=(G')',\ G^{(3)}=(G'')',\cdots,$$
$$G^{(n)}=(G^{(n-1)})',\cdots.$$

$G^{(i)}$称为G的第i导群。证明

$$G\text{是可解群}\iff\text{对某个}k\geqslant 1,\ G^{(k)}=\{e\}.$$

§8 对称群 S_n

在§1的例2、§4的例12及例13中，我们讨论了n个数字的集合$\{1,2,\cdots,n\}$的对称群S_n。与定理2.11相联系的，我们有如下的引理(参考定理2.11后的讨论)。

引理1 任何忠实地作用在集合$N=\{1,2,\cdots,n\}$上的变换群G皆可理解成S_n的子群。详言之，即有一群单射

$$\rho:\ G\to S_n,$$

使得

$$g(i)=\rho(g)(i),\quad \forall g\in G,\ i\in N.$$

证明 已知g作用在N上是一个单满映射，而S_n为N到N的单满映射的集合，就取此单满映射为$\rho(g)$。其余读者自证。▌

系 设一有限群G的阶为n，则有一群单射

$$\rho:\ G\to S_n.$$

即G可以理解为S_n的子群。

定理2.23 群S_n是由$\{(1,2),(1,3),\cdots,(1,n)\}$生成的。

证明 如果$n=1$，则S_n是幺群，由空集生成。如果$n=2$，显然S_2是由$\{(1,2)\}$生成的。用数学归纳法，设S_{n-1}是由$\{(1,2),(1,3),\cdots,(1,n-1)\}$生成的。令$\rho\in S_n$，则有两种可能：$\rho(n)=n$或$\rho(n)=i\neq n$。若$\rho(n)=n$，即$\rho$不变动$n$，则$\rho$可视为$\{1,2,\cdots,n-1\}$上的变换，也即$\rho$可视为$S_{n-1}$的元素。根据数学归纳法，$\rho$可由$\{(1,2),(1,3),\cdots,(1,n-1)\}$生成。若$\rho(n)=i\neq n$，令

$$\sigma=(1,n)*(1,i)*\rho,$$

即

$$\rho=(1,i)*(1,n)*\sigma.$$

显然，

$$\sigma(n)=(1,n)*(1,i)*\rho(n)$$
$$=(1,n)*(1,i)(i)=(1,n)(1)=n,$$

故 σ 可由 $\{(1,2),(1,3),\cdots(1,n-1)\}$ 生成，于是 ρ 可被 $\{(1,2),(1,3),\cdots,(1,n)\}$ 生成。❙

在例12中，我们已经证明了 $\mathrm{Inn}(S_n)$ 即 S_n。以下我们有关于 $\mathrm{Aut}(S_n)$ 的定理。

定理2.24 设 $n\neq 6$，则有 $\mathrm{Aut}(S_n)=\mathrm{Inn}(S_n)$，而

$$[\mathrm{Aut}(S_6):\mathrm{Inn}(S_6)]\leqslant 2.$$

（实际上，上面的不等式是等式，即 S_6 有一非内自同构的自同构，不过其构造方法比较复杂，所以略去不谈。）

证明 $n=1,2$ 的情形是很简单的，所以略去。我们以下讨论 $n\geqslant 3$ 的情形。为了眉目清晰起见，我们分成以下几条：

1） 令 $\sigma\in S_n$，$\mathrm{Orb}(\sigma)$ 表示共轭类，即 σ 在 $\mathrm{Inn}(S)$ 作用下的轨道。设 $\pi\in\mathrm{Aut}(S_n)$，如 $\pi(\sigma)\in\mathrm{Orb}(\sigma_1)$，则 π 把 $\mathrm{Orb}(\sigma)$ 的元素完全映射入 $\mathrm{Orb}(\sigma_1)$。证明如下：

设 $\rho*\sigma*\rho^{-1}$ 为 $\mathrm{Orb}(\sigma)$ 中的任意元素，则有

$$\pi(\rho*\sigma*\rho^{-1})=\pi(\rho)*\pi(\sigma)*\pi(\rho^{-1})$$
$$=\pi(\rho)*\pi(\sigma)*\pi(\rho)^{-1}.$$

即此元素与 $\pi(\sigma)$ 共轭，也即在 $\mathrm{Orb}(\sigma_1)$ 中。

2） 如一自同构 π 把 $\mathrm{Orb}(\sigma_1)$ 映入 $\mathrm{Orb}(\sigma_2)$，则 π 的逆自同构 π^{-1} 把 $\mathrm{Orb}(\sigma_2)$ 映入 $\mathrm{Orb}(\sigma_1)$。π 与 π^{-1} 皆为单射，故知 $\mathrm{Orb}(\sigma_1)$ 与 $\mathrm{Orb}(\sigma_2)$ 的基数相同。

3） 易于看出，

$$\sigma^n=e\implies\pi(\sigma)^n=e,$$
$$\pi(\sigma)^m=e\implies\sigma^m=\pi^{-1}(\pi(\sigma))^m=e.$$

于是在同构的作用下，一元素的阶是不变的。

考虑 S_n 中二阶元素的集合，这是 $\mathrm{Inn}(S_n)$ 作用下的一个不变集合。这个不变集合又是 $\mathrm{Orb}(\delta_i)$ 的并集，δ_i 的定义如下：

$$\delta_i=(1,2)(3,4)\cdots(2i-1,2i).$$

自然，此处 i 受了$2i\leqslant n$的限制(参见例12)。

4) $\mathrm{Orb}(\delta_i)$的基数是什么？在 i 个括号中排入 n 个数字$\{1,2,\cdots,n\}$中的 $2i$ 个，并且允许同一括号中的两个数字调换，也允许括号互换，因而 $\mathrm{Orb}(\delta_i)$ 的基数为

$$\frac{n(n-1)\cdots(n-2i+1)}{i!\,2^i}.$$

于是可知，当 $\mathrm{Orb}(\delta_1)$ 与 $\mathrm{Orb}(\delta_i)$ 的基数相同时，则有 $i=1$ 或 $n=6$，$i=3$。根据以上的讨论，一个自同构 π 必然把 $\mathrm{Orb}(\delta_1)$映入$\mathrm{Orb}(\delta_1)$，或在 $n=6$ 时，把 $\mathrm{Orb}(\delta_1)$映入$\mathrm{Orb}(\delta_3)$。

5) 欲证如 ρ: $\mathrm{Orb}(\delta_1)\to\mathrm{Orb}(\delta_1)$，则 ρ 必为S_n的一个内自同构。如此，则知在$n\neq 6$时，$\mathrm{Aut}(S_n)=\mathrm{Inn}(S_n)\cong S_n$。

设 $l\neq 2$。因为 $(1,2)(1,l)(1,2)=(2,l)$，故

$$\rho(1,2)\rho(1,l)\rho(1,2)=\rho(2,l).$$

但$\rho(1,l)\neq\rho(2,l)$，所以 $\rho(1,2)$与$\rho(1,l)$的轨道式中必有一共同的数，令此数为1_ρ。设另一数$t\neq l,2$，则不难证出 $\rho(1,t)$的轨道式中也必有此数 1_ρ。同法可以求出 $2_\rho,\cdots,n_\rho$。于是有 $\rho(i,j)=(i_\rho,j_\rho)$。根据定理2.23，$\{(1,2),(1,3),\cdots,(1,n)\}$是 S_n 的生成元集。由此不难证出

$$\rho((i,\cdots)*\cdots*(j,\cdots))=(i_\rho,\cdots)*\cdots*(j_\rho,\cdots).$$

参照例 12，可知 ρ 是 S_n的一内自同构。

6) 考虑S_6。取$\mathrm{Aut}(S_6)$的任意两个把$\mathrm{Orb}(\delta_1)$映入$\mathrm{Orb}(\delta_3)$的元素ρ,δ。则有

$$\rho^{-1}*\delta:\ \mathrm{Orb}(\delta_1)\to\mathrm{Orb}(\delta_1),$$

也即ρ与σ属于$\mathrm{Aut}(S_6)$对$\mathrm{Inn}(S_6)$的同一陪集。故有

$$[\mathrm{Aut}(S_6):\mathrm{Inn}(S_6)]\leqslant 2. \quad \blacksquare$$

以下的讨论，除对群论本身有意义外，并对域论的伽罗瓦理论有应用价值。

定义2.22 令$X_1,X_2,\cdots,X_n$为 n 个变数，

$$f=\prod_{n\geqslant i>j\geqslant 1}(X_i-X_j).$$

设$\sigma\in S_n$，σ作用于f如下：

$$\sigma f=\prod_{n\geqslant i>j\geqslant 1}(X_{\sigma(i)}-X_{\sigma(j)}).$$

如果$\sigma f=f$，则称σ为**偶变换**. 如果$\sigma f=-f$，则称σ为**奇变换**.

不难看出，S_n的一元素σ，如非奇变换，则必是偶变换. 并且奇偶性遵守以下的规则：

(奇变换)$*$(奇变换)=(偶变换)，

(奇变换)$*$(偶变换)=(奇变换)，

(偶变换)$*$(奇变换)=(奇变换)，

(偶变换)$*$(偶变换)=(偶变换).

于是奇变换的逆元素为奇变换，偶变换的逆元素为偶变换. 我们有如下之定理.

定理2.25 S_n的所有偶变换构成一子群A_n，称为**交代群**. $[S_n:A_n]=2$. A_n是S_n的正规子群.

证明 $e\in A_n$，所以A_n非空. 如ρ及σ在A_n中，则σ^{-1}及$\rho*\sigma^{-1}$皆在A_n中. 故A_n是一子群.

显然，$(n-1,n)$是一奇变换. 令α为任意奇变换，则$(n-1,n)*\alpha$为一偶变换，即在A_n中. 于是$\alpha\in(n-1,n)*A_n$，故得

$$[S_n:A_n]=2.$$

令$\alpha\in S_n$，则有$\tau_\alpha(A_n)=\alpha*A_n*\alpha^{-1}$为偶变换的集合. 于是有$\tau_\alpha(A_n)\subset A_n$. 所以$A_n$是正规子群. ∎

根据上定理，S_n中有一正规群列$S_n\rhd A_n\rhd\{e\}$，而且S_n/A_n是一单群. 欲将此正规群列细化成S_n的一合成群列，则不外乎构造A_n的一合成群列. 我们先证一引理.

引理 2 A_n是形如(i,j,k)的元素生成的.

证明 A_1与A_2皆幺群，$A_3=\{e,(1,2,3),(3,2,1)\}$. 显然此

引理成立。设$n\geqslant 4$，其证明与定理2.23的证明很近似。设$\sigma\in A_n$，则有两种可能

$$\sigma(n)=\begin{cases}n,\\ i\neq n.\end{cases}$$

在第一种情形，σ可以理解成A_{n-1}内的元素，按照数学归纳法，σ可由形如(i,j,k)的元素累次运算得出。在第二种情形，令

$$\rho=(j,i,n)*\sigma,\quad \sigma=(n,i,j)*\rho.$$

则有$\rho(n)=n$。于是归还成第一种情形。▌

定理2.26 除$n=4$外，A_n皆单群。

证明 A_1,A_2皆幺群，$A_3=\{e,(1,2,3),(1,3,2)\}$，其阶数是素数3。因此除去幺群及本身外，无任何子群，自然是一单群。

以下我们假设$n\geqslant 5$。设N为A_n之一非幺群的正规子群。欲证$N=A_n$。按照上面的引理，只要证明形如(i,j,k)的元素皆在N中便足够了。

令ρ为N之非幺元素中其非幺轨道式的并集为最小者，换言之，ρ变动的数字最少。我们首先证明ρ的轨道式必为(i,j,k)之形。

如果ρ的非幺轨道的基数不同，如下式：

$$\rho=(a_1,\cdots,a_m)(b_1,\cdots,b_l)\cdots.$$

设$m<l$，则ρ^m不变动$a_1,\cdots,a_m$，而且非幺元。这是不可能的。令ρ的非幺轨道的共同基数是m，即

$$\rho=(a_1,\cdots,a_m)(b_1,\cdots,b_m)\cdots(d_1,\cdots,d_m).$$

这有两种可能：$m\geqslant 3$或$m=2$。在第一种情形下，如$m>3$或有两个以上的非幺轨道，则可得出一矛盾如下：令

$$\sigma=(a_1,a_2)*\rho*(a_1,a_2)^{-1}=(a_2,a_1,a_3,\cdots)(\cdots)\cdots,$$

则有$\sigma*\rho(a_1)=a_1$，$\sigma*\rho\neq e$。即$\sigma*\rho$变动的数字更少，所以是不可能的。于是在第一种情形下，$\rho=(a_1,a_2,a_3)$。在第二种情形下，ρ可以写成

$$\rho=(c_1,c_2)(c_3,c_4)\cdots(c_{2r-1},c_{2r}).$$

又可分为两类来讨论：$r\geqslant3$或$r=2$。若$r\geqslant3$，令

$$\sigma=(c_1,c_2,c_3)*\rho*(c_1,c_2,c_3)^{-1}$$
$$=(c_2,c_3)(c_1,c_4)(c_5,c_6)\cdots(c_{2r-1},c_{2r}).$$

则有$\sigma*\rho=(c_1,c_3)(c_2,c_4)$。因此$\sigma*\rho$变动的数字更少，所以不可能。我们仅剩下$r=2$需要考虑了。因为$n\geqslant5$，所以必有一数字$c_5\neq c_1,c_2,c_3,c_4$。令

$$\sigma=(c_1,c_2,c_5)*\rho*(c_1,c_2,c_5)^{-1}=(c_2,c_5)(c_3,c_4),$$

则有$\sigma*\rho=(c_1,c_5,c_2)$.因此$\sigma*\rho$变动的数字更少,所以不可能.

综上所述，我们已证得N中有一形如(i,j,k)的元素。不妨假定此元素即$(1,2,3)$。取任意的$i\neq j$，$i,j\neq1,2,3$，则有

$$(1,i,j)*(1,2,3)*(1,i,j)^{-1}=(i,2,3),$$

即不动$(1,2,3)$中之2及3，可以把1换成i。同法可把2换成j，3换成k。于是N中有所有形如(i,j,k)的元素。▎

系 如$n\neq4$，则$S_n\rhd A_n\rhd\{e\}$是S_n的合成群列。

“可解群”的概念来自用根式“解”代数方程。详情见伽罗瓦理论。下面这个定理是证明五次与更高次方程式不能用根式求解的群论基石。

定理2.27 如$n\geqslant5$，则S_n不是可解群。如$n\leqslant4$，则S_n是可解群。

证明 设$n\geqslant5$，不难看出，S_n的正规群列的长非1即2，其商群集非$\{S_n\}$即$\{S_n/A_n,A_n\}$。因此只需证明A_n非交换群便已足够了。显然有

$$(1,2,3)(2,3,4)=(1,2)(3,4)\neq(1,3)(2,4)$$
$$=(2,3,4)(1,2,3).$$

其次，$S_2\rhd\{e\}$，$S_3\rhd A_3\rhd\{e\}$，其商群集皆为交换群集。因此S_2,S_3为可解群。只余$n=4$的情形了。令

$$K=\{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}.$$

则K是在内自同构作用下两个轨道的并集，所以是一个不变子集。不难看出，K是A_4的正规子群。于是

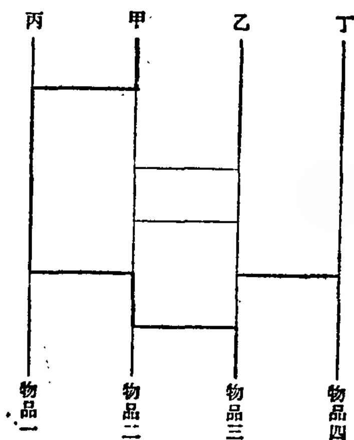
$$S_4 > A_4 > K > \{e\}$$

是S_4的一个正规群列，而其商群集是一交换群集。∎

习　题

1. 证明n个文字的任一置换在分解成对换（即(i,j)）的乘积时，分解出的对换的个数的奇偶性与分解无关。并证明一个置换是奇置换当且仅当它分解出对换的个数是奇数。

2. 考虑下述的"画鬼脚"的游戏：n个人分配n个物品（食物、工作等）的方法。在一张纸上画n条互相平行的竖直线，再在这些竖直线之间画上几条不同高度的连结横线。在竖线下端分别写好要分配的物品的名称。将横线部分遮盖住。让每个人自由地选择上方的线头，打开横线的遮盖物。每个人都沿竖线往下走，但遇到横线必须转向。如此到达的终点处标明的物品即归该人所有。如左图所示。粗线表示甲的行程，所以甲得物品三。不难看出乙得物品四，丙得物品一，丁得物品二。证明：



题2图

(1) 任何"鬼脚"都是一一对应。换句话说，不可能有两个人走到同一个终点，以致发生争执。

(2) 任何一一对应都可由"鬼脚"表出。

3. 证明A_n是S_n的唯一的指数为2的子群。

4. 找出S_4中所有与S_3同构的子群。

5. 找出S_7中的一个最大阶的元素。

6. $(1,2,3,4,5)$在S_5中所在的共轭类的基数是多少？

7. 证明S_n可以由$(1,2)$及$(1,2,\cdots,n)$生成。

8. 设有n个文字$x_1,x_2,\cdots,x_n$，又设$y_1,y_2,\cdots,y_{n-2}$是$x_1,x_2,\cdots,x_{n-2}$的任一排列。证明必存在$\sigma\in A_n$，使得

$$\sigma(x_i)=y_i\ (\forall i=1,2,\cdots,n-2)。$$

9. 证明60阶非交换单群必和A_5同构。

第三章 多 项 式

§1 域 与 环

常见的实数一元多项式集 $\boldsymbol{R}[x]$是形如

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

的元素的集合，其中系数 a_i 皆取自实数集 $\boldsymbol{R}$。在近世代数学中，我们研究类似的元素 $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ 的集合，而系数 a_i 可取自一广义的"域"或"环"。为此，我们定义"域"与"环"如下。

定义3.1 设K为一有两种双项运算"+"(称为加法)及"·"(称为乘法)的集合。如K对"+"而言，是一交换群，其幺元记为0。令

$$K^* = K\backslash\{0\} = \{k: k\in K, k\neq 0\}.$$

如 K^* 对"·"而言，也是一交换群，其幺元记为1。又如K对"+"与"·"而言，满足分配律：

$$a\cdot(b+c) = a\cdot b + a\cdot c, \qquad (b+c)\cdot a = b\cdot a + c\cdot a,$$

此处 a，b，c 是K的任意三元素，则称K是一域。

讨论 1）形象的说，域是可以进行通常的四则运算的集合。代数学常通过对运算的研究，以求了解集合的数学性质。因此，在代数学看来，域K常有实数集 $\boldsymbol{R}$ 的许多数学性质。

2）设K为一域，则K及 K^* 皆为群，所以皆非空集。于是K必有两个不同的元素0及1，$0\neq 1$。即K的基数最少为2。

3）设K为一域，$a\in K$。试问 $0\cdot a=$？$a\cdot 0=$？按照分配律，得出

$$0\cdot a = (0+0)\cdot a = 0\cdot a + 0\cdot a.$$

运用K对加法是一群的性质，在上式中两边消去$0\cdot a$，得

$$0=0\cdot a.$$

同理可证

$$0=a\cdot 0.$$

于是K对乘法而言，是服从交换律的，即

$$a\cdot b=b\cdot a,\qquad \forall a,b\in K.$$

例1 有理数集$\boldsymbol{Q}$、实数集$\boldsymbol{R}$、复数集$\boldsymbol{C}$皆是域。整数集$\boldsymbol{Z}$不是域，因为$\boldsymbol{Z}^*$中，除$+1$与-1外，皆无逆元。

考虑$\boldsymbol{Z}_n$。我们可证，$\boldsymbol{Z}_n$为域的充要条件是n为一素数。证法如下：

显然，对加法而言，$[0]_n$是幺元。$(\boldsymbol{Z}_n)^*=\boldsymbol{Z}_n\backslash[0]_n$。如$n$非素数，令$n=ab$，$0<a<n$，$0<b<n$。则有$[a]_n,[b]_n\in(\boldsymbol{Z}_n)^*$。而

$$[a]_n\cdot[b]_n=[ab]_n=[n]_n=[0]_n\overline{\in}(\boldsymbol{Z}_n)^*,$$

故知$\boldsymbol{Z}_n^*$不可能对乘法成为一群。所以$\boldsymbol{Z}_n$也不可能是一域。

如n为素数，取$(\boldsymbol{Z}_n)^*$的任意元素$[m]_n$，则有$n\nmid m$。于是，n,m的最大公因数必为1。按照定理1.2，有整数b_1及b_2，使得$b_1m+b_2n=1$。取同余式，得

$$[b_1]_n\cdot[m]_n=[1]_n.$$

不难看出，$[1]_n$是$(\boldsymbol{Z}_n)^*$的乘法的幺元，因而$[b_1]_n$是$[m]_n$的逆元。参考定理1.4，易证在此种情形下，即n为素数时，$\boldsymbol{Z}_n$是一域。

以上证完n为素数是$\boldsymbol{Z}_n$为域的充要条件。

值得注意的是，$\boldsymbol{Z}_n$的基数是n。这是一个有限数。凡域K的基数为有限数时，则域K称为**一有限域**。 ▎

从以上的讨论及例子中，我们看出“域”是许多优良的数学集合的“共名”。然而也有许多优良的数学集合，如$\boldsymbol{Z},\boldsymbol{Z}_4$等，不在此限内。于是我们又有另一较广泛的“共名”，即“环”。其定义如下。

定义3.2 设R为一有两种双项运算“+”（称为加法）及

“·”(称为乘法)的集合。如R对“+”而言，是一交换群；R对“·”而言，有幺元1并有结合律，即取任意三元素a,b,c,有

$$a\cdot(b\cdot c)=(a\cdot b)\cdot c。$$

又如R对“+”及“·”而言，满足分配律：

$$a\cdot(b+c)=a\cdot b+a\cdot c,\qquad (b+c)\cdot a=b\cdot a+c\cdot a,$$

则称R是一**环**。如R是一环，并且其乘法适合交换律，则称R为一**交换环**。

讨论 1) 在许多书本中，并不要求“环”中有乘法的幺元。于是这些书中,称有乘法的幺元的环为“有幺元(或有单位)的环”。实际上这些书中的绝大多数的环皆有乘法的幺元。“有幺元的环”这个名词实嫌啰嗦，本书采用另一种命名法，规定凡环中皆有乘法的幺元。如一集合R，除了无乘法的幺元之外，有环的其它的特性，则称R为一**无幺元的环**。

2) 如R仅有一个元素，则此元素必为加法的幺元0。此环R称为**零环**。

3) 设R是一交换环。如二非零元素a，b的乘积是0，即

$$a\neq 0,\qquad b\neq 0,\qquad a\cdot b=0,$$

则称a,b为**零因子**，如R是基数大于1的交换环，而且没有零因子，则称R为一**整环**。

4) 设R为一非零环。如$a,b\in R$，使$b\cdot a=a\cdot b=1$，则称b是a的**逆元**，a是b的**逆元**，a,b是**可逆元**。参照第二章§1，不难看出，一可逆元a的逆元是唯一的，以a^{-1}表示之。

5) 环R的子集S如果含有R的乘法幺元1，而且对R的加法及乘法构成环，则称S是R的**子环**。

例2 任意域K皆是整环。这因为$a\neq 0,b\neq 0$，则$a,b\in K^*$，所以$a\cdot b\in K^*$，即$a\cdot b\neq 0$。于是，有理数集$\boldsymbol{Q}$、实数集$\boldsymbol{R}$、复数集$\boldsymbol{C}$等皆是整环。

不难看出，整数集$\boldsymbol{Z}$是一整环。按照定理1.4，$\boldsymbol{Z}_n$是交换环。更进一步说，如n非素数，令

$$n=a\cdot b,\quad 0<a<n,\ 0<b<n,$$

则有

$$[a]_n\neq 0,\quad [b]_n\neq 0,\quad [a]_n[b]_n=[n]_n=0.$$

于是 $\boldsymbol{Z}_n$ 不是整环。

所有偶数的集合 $2\boldsymbol{Z}=\{2m:\ m\in\boldsymbol{Z}\}$ 是一"无幺元的环"。同理，当 $n>1$ 时，$n\boldsymbol{Z}=\{nm:\ m\in\boldsymbol{Z}\}$ 也是"无幺元的环"。

例 3 有限域——如 $\boldsymbol{Z}_p$ (p 为素数) 等——是比较抽象的数系，然而也很有应用价值。我们试取一例：一般电码是由 0，1 两数组成，相当于电源的开、关。一般在收、发电码时，由于干扰及人为错误等等，不免产生误码。补救的办法之一是每个电码皆连发两次。例如一个四数的电码

$$a_1\,a_2\,a_3\,a_4,$$

假定最多只有一个误码，则可以发成

$$a_1\,a_1\,a_2\,a_2\,a_3\,a_3\,a_4\,a_4,$$

此处 a_1,a_2,a_3,a_4 皆是 0 或 1。如果此八个数皆两两相等，则知电码无误。然而如果某处的两数不等，则知电码有误，但也不能知道原电码究竟是 0 还是 1。如果要进一步知道原电码，势必每一数皆连发三次

$$a_1\,a_1\,a_1\,a_2\,a_2\,a_2\,a_3\,a_3\,a_3\,a_4\,a_4\,a_4.$$

此时，每一组的三个数，如不尽相同，则可认定 0，1 中出现两次的是原电码。读者立刻看出，这种方法要增加两倍的工作量。能不能利用"有限域"的方法，巧妙地减少工作量呢？解法如下。

考虑 $\boldsymbol{Z}_2=\{[0]_2,[1]_2\}$。为了简化写法起见，令 $0=[0]_2$，$1=[1]_2$。于是

$$0+1=1+0=1,\quad 0+0=0,\quad 1+1=0,$$

$$0\times 1=1\times 0=0\times 0=0,\quad 1\times 1=1.$$

考虑

$$\boldsymbol{Z}_2\oplus\boldsymbol{Z}_2\oplus\boldsymbol{Z}_2\oplus\boldsymbol{Z}_2\oplus\boldsymbol{Z}_2\oplus\boldsymbol{Z}_2\oplus\boldsymbol{Z}_2=(\boldsymbol{Z}_2)^7$$
$$=\{(a_1,a_2,a_3,a_4,b_1,b_2,b_3):\ a_i,b_i\in\boldsymbol{Z}_2\}.$$

有些读者知道这是“以 $\boldsymbol{Z}_2$ 为数系的七维空间”。但是，这个概念暂时是无关紧要的，所以目前不懂也无妨。

取下列的矩阵 A：

$$A=\begin{pmatrix}1&1&1\\1&1&0\\1&0&1\\0&1&1\\1&0&0\\0&1&0\\0&0&1\end{pmatrix},$$

以 $v=(a_1,a_2,a_3,a_4,b_1,b_2,b_3)$ 与 A 相乘，乘法的定义是一般向量与矩阵的乘法，即

$$v\cdot A=(u_1,u_2,u_3),$$
$$u_1=a_1+a_2+a_3+b_1,$$
$$u_2=a_1+a_2+a_4+b_2,$$
$$u_3=a_1+a_3+a_4+b_3.$$

给定任意电码 a_1,a_2,a_3,a_4，求得辅助性的 b_1,b_2,b_3，使 $u_1=u_2=u_3=0$，即

$$-b_1=a_1+a_2+a_3,\quad -b_2=a_1+a_2+a_4,\quad -b_3=a_1+a_3+a_4.$$

然后，发出电码 $a_1,a_2,a_3,a_4,b_1,b_2,b_3$。收电码的人，将收得的电码 $v'=(a'_1,a'_2,a'_3,a'_4,b'_1,b'_2,b'_3)$ 与矩阵 A 相乘，得

$$v'\cdot A=(u'_1,u'_2,u'_3).$$

如 $u'_1=u'_2=u'_3=0$，则知电码无误。如有一处错误，则以 (u'_1,u'_2,u'_3) 与矩阵 A 的各行相比较。相同者的行数即错误电码的序数。例如，设 $(u'_1,u'_2,u'_3)=(1,0,1)$，则知 a_3 有错。于是将误码进行 0，1 互换，即可以改正其错误。什么道理呢？我们假定，电

码不容易发生误码，这七个电码中，最多只有一个误码。于是可设只在 i 处电码与原码不符，则有

$$v' = v + (0,\cdots,0,1,0,\cdots,0).$$

而

$$\begin{aligned} v'\cdot A &= v\cdot A + (0,\cdots,0,1,0,\cdots,0)\cdot A \\ &= 0 + (0,\cdots,0,1,0,\cdots,0)\cdot A \\ &= A\text{的第 } i \text{ 行}, \end{aligned}$$

于是 i 即电码错误之处。

很容易推广上面的办法。可取 A 是一 n 列 2^n-1 行的矩阵。令 $m=2^n-1-n$，则可一次发出 m 个电码 $a_1,a_2,\cdots,a_m$；另取 $b_1,b_2,\cdots,b_n$ 为辅助性的电码，发出电码 $a_1,a_2,\cdots,a_m,b_1,b_2,\cdots,b_n$。利用上面的数学关系，收电码的人不仅可以发现一个错误，而且可以改正这个错误。取 $n=4$ 时，$m=11$。取 $n=5$时，$m=26$等等。如电码相当精确，只会偶而出错，那么这个方法可以节省大量的人力物力。

读者应试行写出 $n=4$，$m=11$时的矩阵 A 及完成其讨论。

习　题

1. 在全体 $n\times n$ 实矩阵所成的集合 $FL(n,R)$中，定义其加法与乘法为普通矩阵的加法与乘法，证明它是一个环，这个环不是交换环。

2. 续上题。证明环 $FL(n,R)$中有零因子，即 $A\neq 0, B\neq 0$，但 $AB=0$。

3. 闭区间$[0,1]$上全体实连续函数所成的集合关于普通函数加法、乘法组成一环，证明这个环有零因子。

4. 设 R 是一个非交换环，$a,b\in R$。如果 $1-ab$ 是 R 的可逆元素，试证明 $1-ba$ 也是 R 的可逆元素。

5. 设 a,b 是环 R 的两个元素，$a,b,ab-1$都可逆，试证明 $a-b^{-1}$ 和 $(a-b^{-1})^{-1}-a^{-1}$ 也可逆，且

$$[(a-b^{-1})^{-1}-a^{-1}]^{-1}=aba-a.$$

6. 证明在环的定义中，加法的交换律可由其它公理推导出。

7. 证明集合

$$\mathbf{Q}(\sqrt[3]{2})=\{a+b\sqrt[3]{2}+c\sqrt[3]{4}:\ a,b,c\in\mathbf{Q}\}$$

关于实数的加法、乘法组成一个域，在此域中，试求出 $-2+\sqrt[3]{2}+3\sqrt[3]{4}$ 的逆元素。

8. 证明集合

$$C=\left\{\begin{bmatrix} a & b \\ -b & a \end{bmatrix}:\ a,b\in\mathbf{R}\right\}$$

关于矩阵加法与乘法组成一个域。

9. 参看例3，写出 $n=4,m=11$ 时的矩阵 A。设一个电码的错误的或然率是十万分之一，讨论此时电码错误的或然率。

10. 域的特征。设 k 是域，1是 k 的乘法幺元。如果

$$\overbrace{1+1+\cdots+1}^{n\text{项}}=0,$$

而少于 n 个1相加永不为零，我们定义 k 的**特征**为 n。如没有这样的 n 存在，我们定义 k 的**特征**为零。证明：如 k 的特征不为零时，它必为一素数。

11. 设域 k 的特征 $p\neq 0$，那么任取 $a,b\in k$，我们恒有

$$(a+b)^p=a^p+b^p.$$

12. 令 $R_i(i\in I)$ 是环，我们定义**直和**(direct sum)

$$\bigoplus_{i\in I}R_i=\{(\cdots,r_i,\cdots):\ r_i\in R_i,\ \text{只有有限个}r_i\text{不为零}\},$$

其元素的加法和乘法定义如下：

$$(\cdots,r_i,\cdots)+(\cdots,s_i,\cdots)=(\cdots,r_i+s_i,\cdots),$$

$$(\cdots,r_i,\cdots)(\cdots,s_i,\cdots)=(\cdots,r_is_i,\cdots).$$

证明此时 $\bigoplus_{i\in I}R_i$ 成一环，当指标集 I 的基数≥2时，这个环不是整环。

13. 令 $R_i(i\in I)$ 是环，我们定义**直积**(direct product)

$$\prod_{i\in I} R_i = \{(\cdots, r_i, \cdots):\ r_i \in R_i\},$$

其加法、乘法的定义与题12同。证明$\prod_{i\in I} R_i$是一个环。

14. **群环（group ring）**。设R是环，G是群。令

$R[G] = \{\sum r_i g_i:\ r_i \in R,\ g_i \in G$,其中只有限个$r_i$不为0$\}$。

定义

$$\sum r_i g_i + \sum s_i g_i = \sum (r_i + s_i) g_i,$$

$$\left(\sum_i r_i g_i\right)\left(\sum_j s_j g_j\right) = \sum_k \left(\sum_{g_i g_j = g_k} r_i s_j\right) g_k.$$

证明上面的定义是良好的，它使$R[G]$成为一个环。

§2 多项式环及比域

我们首先把实数一元多项式推广到系数取自一环R的一元多项式。

定义3.3 设R为一环，x为一变数。系数取自环R的**一元多项式环**$R[x]$，即是集合

$$\left\{\sum_{\text{有限}} a_i x^i:\ i\ \text{为非负整数},\ a_i \in R\right\}$$

（x^0定义为1），且有如下定义的加法及乘法：

1） $\sum_i a_i x^i + \sum_j b_j x^j = \sum_k (a_k + b_k) x^k$；

2） $\left(\sum_i a_i x^i\right)\cdot\left(\sum_j b_j x^j\right) = \sum_n \left(\sum_{i+j=n} a_i b_j\right) x^n$。

讨论 1）不难看出$R[x]$是一环，其加法的幺元是R的加法幺元0，其乘法幺元是R的乘法幺元1。

2） $R[x]$也称为环R的一元多项式环。如果变数x在讨论中有特殊的意义时，则可称$R[x]$为环R的以x为变数的一元多项式环。相对于一元多项式环$R[x]$而言，R可称为其常数环。

3） 如果R为交换环，则$R[x]$也为交换环。∎

整系数一元多项式及有理系数一元多项式的起源很古。在古中国、巴比伦、埃及、希腊的数学中，皆有一次及二次多项式的讨论。多项式环是代数学的基石之一，我们且举一些实例。

例 4 整数一元多项式环$\mathbf{Z}[x]$，有理数一元多项式环$\mathbf{Q}[x]$，实数一元多项式环$\mathbf{R}[x]$，复数一元多项式环$\mathbf{C}[x]$，及$\mathbf{Z}_n[x]$等等。

如取$R=\mathbf{Q}[x]$，则定义$\mathbf{Q}[x,y]=R[y]$。此处x，y为两个不相关的变数。于是

$$\mathbf{Q}[x,y]=\left\{\sum_j\left(\sum_i a_{ij}x^i\right)y^j:\ i,j\text{ 取有限个非负整数},\ a_{ij}\in\mathbf{Q}\right\}$$

$$=\left\{\sum_{j,i}a_{ij}x^iy^j:\ i,j\text{ 取有限个非负整数},\ a_{ij}\in\mathbf{Q}\right\},$$

即为有理数的二元多项式环。同理，任取一环R及不相关的n个变数$x_1,x_2,\cdots,x_n$，则可定义

$$R[x_1,x_2,\cdots,x_n]=(\cdots((R[x_1])[x_2])\cdots)[x_n],$$

即环R的n元多项式环。

从以上的讨论我们知道，如令$R=\mathbf{Q}[x_1,x_2,\cdots,x_{n-1}]$，则

$$\mathbf{Q}[x_1,x_2,\cdots,x_n]=R[x_n].$$

换言之，n元多项式环可以当成一元多项式环来考虑。于是某些一元多项式环的数学特性是n元多项式环共有的。如此，讨论$R[x_n]$时，已涉及了$\mathbf{Q}[x_1,x_2,\cdots,x_n]$。这是数学的“以简驭繁”的妙用。

例 5 取一变数x。令$u=x-1$，则不难看出，$\mathbf{R}[x]=$

$R[u]$。变数 x 及 u 的区别，是两者的原点不同。如取 x 为实数轴 R 的标准坐标，则 x 的原点自然是 0。而相对于此一标准坐标而言，u 的原点是 $u=0$，即 $x=1$。

取二不相关的变数 x，y，令

$$u=x, \quad v=y+x^2,$$

则不难看出 $R[x,y]=R[u,v]$。令 x，y 为实数平面的标准坐标，则 $x=a$ 与 $y=b$ 给出平面上一些竖直的与水平的直线。相对于此一标准坐标而言，u，v 给出另一坐标系。此一新坐标系即由下列的网格组成

$$u=a \quad 与 \quad v=b,$$

即

$$x=a \quad 与 \quad x^2+y=b.$$

如此得出的坐标线是一些竖直线与一些抛物线。

总而言之，给定一实数 n 元多项式环 A，相当于给定一个 n 维实数空间 R^n。如给定 $A=R[x_1,x_2,\cdots,x_n]$，则给定 R^n 的原点及一坐标系。如给定

$$A=R[x_1,x_2,\cdots,x_n]=R[u_1,u_2,\cdots,u_n],$$

则给定 R^n 中的两个原点，两个坐标系：$(x_1,x_2,\cdots,x_n)$ 及 $(u_1,u_2,\cdots,u_n)$，以及其间的关系。▎

研究多项式环的要点是：1）研究此环的代数构造；2）研究一组多项式的公解，由此得出代数数论及几何学；3）研究此环的代数构造与一组多项式的公解之间的数学联系。近世关于 3）的研究，成果很丰盛，大放异彩，几乎融合代数、几何、代数数论、黎曼曲面等等于一炉而共冶矣。

在此章中，我们将初步地研究 1)，即多项式环的代数构造，及附带地研究 2)。

取一环 R 及一元多项式环 $R[x]$。令 $f(x)=\sum_i a_i x^i \in R[x]$。则 $f(x)$ 有一**次数** $\deg f(x)$ 及其在原点的**阶数** $\mathrm{ord}_x f(x)$。详言之，即如下之定义。

定义3.4 设R为一环，$R[x]$为一元多项式环，

$$f(x)=\sum_i a_i x^i \in R[x].$$

如$f(x)\neq 0$，则

$$\deg f(x)=\max\left\{i:\ f(x)=\sum_i a_i x^i,\quad a_i\neq 0\right\},$$

$$\mathrm{ord}_x f(x)=\min\left\{i:\ f(x)=\sum_i a_i x^i,\quad a_i\neq 0\right\};$$

如$f(x)=0$，则定义$\deg 0=-\infty$，$\mathrm{ord}_x 0=\infty$。

讨论 1) 如令$u=x+a$，则$R[u]=R[x]$，$\deg_u f=\deg_x f$，但常常可能$\mathrm{ord}_u f\neq \mathrm{ord}_x f$。

2) 在多元多项式环中，也可定义"次数"，然而此时次数与变数有关。例如在$\boldsymbol{R}[x,y]$中，可以定义$\deg_{x,y}$。我们试看例5，

$$u=x,\qquad v=y+x^2,\qquad \boldsymbol{R}[x,y]=\boldsymbol{R}[u,v],$$

而

$$\deg_{x,y}v=2\neq 1=\deg_{u,v}v.$$

定理3.1 如R为一整环，则次数$\deg$及阶数ord_x有如下之性质：

1) 取$f(x)\in R[x]$。如$f(x)\neq 0$，则

$$\deg f(x)\geqslant 0,\qquad \mathrm{ord}_x f(x)\geqslant 0;$$

如$f(x)=0$，则

$$\deg f(x)=-\infty,\qquad \mathrm{ord}_x f(x)=\infty.$$

2) 取$f(x),g(x)\in R[x]$。则有

$$\deg(f(x)\cdot g(x))=\deg f(x)+\deg g(x),$$

$$\mathrm{ord}_x(f(x)\cdot g(x))=\mathrm{ord}_x f(x)+\mathrm{ord}_x g(x).$$

3) 取$f(x),g(x)\in R[x]$。则有

$$\deg(f(x)+g(x))\leqslant\max(\deg f(x),\deg g(x)),$$

$$\mathrm{ord}_x(f(x)+g(x))\geqslant\min(\mathrm{ord}_x f(x),\mathrm{ord}_x g(x)).$$

证明 此三点皆甚易证，故证明从略。▎

此定理与定理1.18有关。为了阐明这个关系，我们引入如下的定义。

定义3.5 设S为一交换环。一映射$v: S \to \mathbf{R}$ 如适合下列条件时，则称v为一**赋值**：

1) 取 $a \in S$，则有$v(a) \geqslant 0$，且$v(a)=0 \Longleftrightarrow a=0$；

2) 取 $a,b \in S$，则有$v(a \cdot b)=v(a)v(b)$；

3) 取 $a,b \in S$，则 $v(a+b) \leqslant \max(v(a),v(b))$。

应用赋值的概念，定理3.1可重写如下。

定理3.1* 如R为一整环，设$f(x) \in R[x]$，令

$$v_x(f(x))=2^{-\operatorname{ord}_x f(x)}, \qquad v_{x^{-1}}(f(x))=2^{\deg f(x)},$$

则v_x与$v_{x^{-1}}$皆是赋值。

证明 读者自证。▌

定理3.2 如S为一非零环的交换环，且S中有一赋值v，则S为整环。

证明 设$a,b \in S$，$a \neq 0$，$b \neq 0$。则根据定义3.5，

$$v(a) \neq 0, \qquad v(b) \neq 0,$$

于是$v(a \cdot b)=v(a)v(b) \neq 0$，故$ab \neq 0$。▌

系 如R为一整环，则$R[x_1,x_2,\cdots,x_n]$也为整环。

就像自整数环$\mathbf{Z}$构造有理数域$\mathbf{Q}$一样，从任意整环S也可以用同样的方法建造一"比域"，其定义如下。

定义3.6 设S为一整环。令

$$K=\left\{\frac{a}{b}: a,b \in S,\ b \neq 0,\ \text{如 } a \cdot d=b \cdot c,\ d \neq 0,\right.$$

$$\left.\text{则}\frac{a}{b}=\frac{c}{d}\right\}.$$

K称为S的**比域**(或**分式域**)。在比域K中，定义加法"+"及乘法"·"如下：

$$\frac{a}{b}+\frac{c}{d}=\frac{a \cdot d+b \cdot c}{b \cdot d},$$

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{a\cdot c}{b\cdot d}.$$

讨论 1) 不难看出，比域是一域。比域K的加法的幺元是$0/1$，乘法的幺元是$1/1$。一般言之，如$b=1$，a/b常写成a。这样，则比域K的加法的幺元是0，乘法的幺元是1。如$a=0$，则

$$\frac{a}{b}=\frac{0}{b}=0.$$

如$a\neq 0$，则a/b的乘法逆元素是b/a。

2) 比域K又可以比较严谨地定义如下：取集合S的直积

$$S\times S=\{(a,b):\ a,b\in S\}.$$

于其中取一子集T，

$$T=\{(a,b):\ a,b\in S,\ b\neq 0\}.$$

在子集T中定义一等价关系"～"如下(参考定义1.4*)：

$$(a,b)\sim(c,d)\iff a\cdot d=b\cdot c.$$

读者自证～确为一等价关系。子集T对～取商集，则得比域K。

例6 有理数域$\boldsymbol{Q}$是整数环$\boldsymbol{Z}$的比域。实数一元多项式环$\boldsymbol{R}[x]$的比域是**实数一元有理函数域**$\boldsymbol{R}(x)$。一般言之，设K为域，则$K[x]$的比域是**以K为系数域的一元有理函数域**，通常以$K(x)$表示之。$K[x_1,x_2,\cdots,x_n]$的比域是**以K为系数域的n元有理函数域**，通常以$K(x_1,x_2,\cdots,x_n)$表示之。▌

有理函数域$K(x_1,x_2,\cdots,x_n)$是饶有意义的数学集合。我们取一简单的例子$\boldsymbol{R}(x)$来研究。令

$$h(x)=\frac{f(x)}{g(x)}\in\boldsymbol{R}(x),$$

此处$f(x),g(x)\in\boldsymbol{R}[x]$。如果$x=a$时，$g(a)\neq 0$，则$h(a)\in\boldsymbol{R}$，即$x=a$在$h(x)$的"定义域"内。所以给定$h(x)$后，我们有$h(x)$的定义域。可是$\boldsymbol{R}(x)$中的所有有理函数并无公有的定义域。进

一步言之，任取一点$x=a$，则$\frac{1}{x-a}$不能定义在点$x=a$上。然而任取有限多个有理函数$h_1(x),h_2(x),\cdots,h_m(x)$，则有一公有的定义域，即$h_1(x),h_2(x),\cdots,h_m(x)$的定义域的交集。这个现象是较复杂的，然而也因此使$R(x)$的内容更为丰富。为了处理这个定义域的问题，我们引入以下的“局部化环”的概念。

定义3.7 设S为一整环。

1）S的一非空子集D，如果适合下列两个条件，则称为一**分母系**：(a) $0\notin D$；(b) $d_1,d_2\in D\Longrightarrow d_1\cdot d_2\in D$。

2）设D为一分母系，则S对D的**局部化环**S_D定义为S的比域K中可以表为s/d（此处$s\in S$，$d\in D$）的元素的集合。

讨论 1）不难看出S_D是一整环。

2）在$\boldsymbol{R}[x]$中，令$D=\{f(x):\ f(0)\neq 0\}$，则D是一个分母系，而

$$\boldsymbol{R}[x]_D=\left\{\frac{f(x)}{g(x)}:g(0)\neq 0\right\}.$$

此即定义在原点$x=0$及其附近的有理函数的集合，如果我们仅考虑原点及其附近的“局部”，则此环包含了所有有意义的有理函数。既使在此局部化环内，各有理函数的定义域也仅有一个公共点，即$x=0$。于是，函数的定义域仍随函数而变。

3）在$\boldsymbol{Z}$中，令$D=\{z^n:\ z$为固定非零整数，n为正整数$\}$，则

$$\boldsymbol{Z}_D=\left\{\frac{m}{z^n}:\ n\text{为正整数},\ m\in\boldsymbol{Z}\right\}.$$

4）如果S非一整环，也可以讨论局部化环S_D。此局部化环S_D是很有趣味的，与几何学甚有关系。此种讨论将留到以后的“环论”中进行，目前我们仅限于S是整环的情形。

5）设S为一整环，$D=S\backslash\{0\}$，即D为所有非零元素的集合。则S_D即是S的比域。如果S为任意交换环时，在以后的“环论”中，我们将把比域的概念引伸为“比环”。

习　题

1. 证明$Z_6[x]$不是整环。

2. 试在$Z_5[x]$内定义一赋值v。令

$$f(x)=x^5-2x^3+1.$$

试求一$g(x)\in Z_5[x]$，使

$$v(f-g)\leqslant 10.$$

3. 在环Z内给定下列分母系：

(1) $D=\{1,-1\}$;

(2) $D=\{2k: k\in Z, k\neq 0\}$;

(3) $D=\{2k+1: k\in Z\}$.

试求Z_D。

4. 在环$Z[\mathrm{i}]$内，令$(\alpha)=(-2+\mathrm{i})$，而$D=Z[\mathrm{i}]\backslash(\alpha)$。证明$D$是一个分母系，并问$Z[\mathrm{i}]_D$的元素是什么？

5. 令

$$R=\left\{\sum_{i=1}^{n} a_i x^{r_i}: a_i\in \mathbf{R},\ r_i=\frac{k_i}{2^{m_i}},\ k_i, m_i \text{ 为非负整数}\right\}.$$

证明R关于普通代数式的加法、乘法组成一个整环。

6. 给定域k上的两个非零二元多项式

$$f(x,y)=a_0(x)y^n+a_1(x)y^{n-1}+\cdots+a_n(x),$$
$$g(x,y)=b_0(x)y^m+b_1(x)y^{m-1}+\cdots+b_m(x),$$

其中$a_i(x), b_j(x)\in k[x]$。又设

$$f(x,y)g(x,y)=c_0(x)y^{m+n}+c_1(x)y^{m+n-1}+\cdots+c_{m+n}(x).$$

证明

$$\max_{0\leqslant i\leqslant n}\{\deg a_i(x)\}\leqslant \max_{0\leqslant k\leqslant m+n}\{\deg c_k(x)\}.$$

7. 令$k=Z/5Z$为一有限域，试在$k[x]$内找出两个互不相同的多项式$f(x), g(x)$，使对k中任意元素a，都有

$$f(a)=g(a).$$

8. 形式幂级数环(formal power series ring). 设R是环，我们定义R上的形式幂级数环

$$R[[x]]=\left\{\sum_{i=0}^{+\infty}a_ix^i:\ a_i\in R\right\},$$

其加法与乘法定义如下：

$$\left(\sum_i a_ix^i\right)+\left(\sum_i b_ix^i\right)=\sum_i\left(a_i+b_i\right)x^i,$$

$$\left(\sum_i a_ix^i\right)\left(\sum_j b_jx^j\right)=\sum_k\left(\sum_{i+j=k}a_ib_j\right)x^k.$$

证明$R[[x]]$是一环.

9. 续上题. 任取$f(x)=\sum_i a_ix^i\in R[[x]]$，定义$f(x)$的阶$\operatorname{ord}f(x)$如下：

$$\operatorname{ord}(f(x))=\min\{i:\ a_i\neq 0\}.$$

证明当R是整环时，我们恒有

$$\operatorname{ord}(f(x)g(x))=\operatorname{ord}(f(x))+\operatorname{ord}(g(x)).$$

并由此证明：R是整环$\Longleftrightarrow R[[x]]$是整环.

10. 利用

$$\frac{1}{1-y}=1+y+\cdots+y^n+\cdots$$

的恒等式证明：当R是整环时，$f(x)=\sum_i a_ix^i$是$R[[x]]$的可逆元$\Longleftrightarrow a_0$是R的可逆元.

11. 利用题10证明：当R是域时，

$$f(x)\text{是可逆元}\Longleftrightarrow\operatorname{ord}(f(x))=0.$$

12. 当R是域时，证明$R[[x]]$的比域是形式亚纯函数域

$$R((x))=\left\{\sum_{i=-m}^{+\infty}a_ix^i:\ m\in\mathbf{Z},a_i\in R\right\}.$$

13． 设p是一个素数。证明$D=\{p^n: n=0,1,2,\cdots\}$是$Z$的一个分母系。更进一步，证明$Z_D/Z$的每一个加法真子群都是有限群，而$Z_D/Z$自身不是有限群。

§3 多项式环的唯一分解定理

令K为域（不妨设想$K=Q,R,C$）。欲证n元多项式环$K[x_1,x_2,\cdots,x_n]$中有唯一分解定理。用数学归纳法，设已知$S=K[x_1,x_2,\cdots,x_{n-1}]$中有唯一分解定理，则仅需证$S[x_n]$中有唯一分解定理便可。本节将循此线索进行。读者请参考第一章§2及§5。

定义3.8 设S为一整环。S的元素α,β,γ，如适合$\alpha=\beta\gamma$，则称α为β的**倍元**，β为α的**因元**，用$\beta|\alpha$表示之。如$\beta|\alpha_1,\beta|\alpha_2,\cdots,\beta|\alpha_n$，则称$\beta$为$\alpha_1,\alpha_2,\cdots,\alpha_n$的**公因元**。

定义3.9 设S为一整环，α为S的一非零非可逆的元素。如$\alpha=\beta\gamma$时，必有β,γ之一为可逆元素，则称α为一**不可分解元**（或**不可约元**）。设α_1,α_2为S的任意二元素，如存在$\delta_1,\delta_2\in S$，使$\alpha_1=\delta_2\alpha_2$，$\alpha_2=\delta_1\alpha_1$，则称$\alpha_1,\alpha_2$为**相伴**的元素，以$\alpha_1\overset{a}{\sim}\alpha_2$表示之。

讨论 1）设$\alpha_1\overset{a}{\sim}\alpha_2$。如$\alpha_1=0$，则显然有$\alpha_2=0$。与1相伴的元素，显然是所有的可逆元。设$\alpha_1\neq 0$，$\alpha_1\overset{a}{\sim}\alpha_2$，则有

$$\alpha_1=\delta_2\alpha_2=\delta_2\delta_1\alpha_1.$$

移项后得$\alpha_1(1-\delta_2\delta_1)=0$。因$S$为整环，且$\alpha_1\neq 0$，因此$1-\delta_2\delta_1=0$，即$\delta_2\delta_1=1$，于是$\delta_1,\delta_2$必皆为可逆元。

2）“相伴”显然是一等价关系。于是S被相伴关系$\overset{a}{\sim}$划分成一些等价子集。

3）设$\alpha_1\overset{a}{\sim}\alpha_2$。如$\alpha_1$是可分解元，即存在$\beta,\gamma\in S$，使

$$\alpha_1=\beta\gamma,$$

而β,γ皆非可逆元。则$\alpha_2=\delta_1\alpha_1=(\delta_1\beta)\gamma$，其中$\gamma$自然不是可逆元，且$\delta_1\beta$也必非可逆元。为什么呢？如果$\varepsilon$是$\delta_1\beta$的逆元，则有

$$1 = \varepsilon(\delta_1\beta) = (\varepsilon\delta_1)\beta,$$

即$\varepsilon\delta_1$是β的逆元，与β非可逆元矛盾。故知$\delta_1\beta$非可逆元。综上所述，在相伴的元素中，如有一元素可分解，则其余元素也皆可分解。换言之，与不可分解元相伴的元素必是不可分解元。

4）设S为一整环，则其所有可逆元的集合对乘法而言是一交换群。可逆元的概念适用于一般的非零环，交换环的可逆元的集合也是一乘法交换群。

5）设S为一整环。又设一元多项式$\alpha \in S[x]$为一可逆元。则有$\beta \in S[x]$，使$\alpha \cdot \beta = 1$。考虑此式的次数deg，得

$$\deg(\alpha \cdot \beta) = \deg\alpha + \deg\beta = \deg 1 = 0.$$

于是$\deg\alpha = 0 = \deg\beta$，即$\alpha, \beta \in S$。所以$S[x]$中的可逆元皆是$S$中的可逆元。如取

$$S = K[x_1, x_2, \cdots, x_{n-1}],$$

此处K是域，则知$K[x_1, x_2, \cdots, x_{n-1}, x_n]$中的可逆元的集合是

$$K^* = K\backslash\{0\}.$$

定义3.10 设S为一整环。如取任意非零元素$\alpha \in S$，恒有

1）$\alpha = \delta \prod_{i=1}^{n} p_i^{m_i}$，此处$\delta$为一可逆元，$m_i (i = 1, 2, \cdots, n)$为正整数，$p_1, p_2, \cdots, p_n$为两两不相伴的不可分解元；

2）如$\alpha = \delta \prod_{i=1}^{n} p_i^{m_i} = \varepsilon \prod_{j=1}^{l} q_j^{u_j}$，此处$\delta, \varepsilon$为可逆元，$m_i$，$u_j$为正整数，$p_1, \cdots, p_n$是两两不相伴的不可分解元，$q_1, \cdots, q_l$是两两不相伴的不可分解元，则$n = l$，且经过重新把$q_1, \cdots, q_l$编号后，必有

$$p_i \overset{a}{\sim} q_i, \quad m_i = u_i, \quad \forall i = 1, 2, \cdots, n.$$

那么，称S为**唯一分解的整环**。

讨论 1）任意域K中非零元素皆是可逆元，故无不可分解

元存在，于是域K是唯一分解的整环。

2）欲证一整环S中有唯一分解定理，即证此整环S是唯一分解的整环。

3）根据第一章的§2及§5，我们已知$\mathbf{Z}$及$\mathbf{Z}[\mathrm{i}]$是唯一分解的整环。

4）有许多整环并非唯一分解的整环。我们试取一例：令

$$S=\mathbf{R}[x^2,x^3]=\left\{\sum_i a_i x^i \in \mathbf{R}[x]:\ a_1=0\right\}.$$

请读者注意$x \notin S$。不难看出x^2,x^3是S的不相伴的不可分解元，而

$$x^6=(x^2)^3=(x^3)^2.$$

所以S并非唯一分解的整环。

定义3.11 设S为一整环，$d,a_1,a_2,\cdots,a_n$为其元素。如有

1）$d|a_1$，$d|a_2$，$\cdots$，$d|a_n$；

2）当$d_1|a_1$，$d_1|a_2$，$\cdots$，$d_1|a_n$时，必有$d_1|d$，

则称d是$a_1,a_2,\cdots,a_n$的一个**最大公因元**。用符号$\mathrm{G.C.D}(a_1,a_2,\cdots,a_n)$表示$a_1,a_2,\cdots,a_n$的最大公因元的集合。

讨论 1）如果d是$a_1,a_2,\cdots,a_n$的一个最大公因元，则另一元素d'也是$a_1,a_2,\cdots,a_n$的一个最大公因元的充要条件是$d\overset{a}{\sim}d'$。

2）如果S并非唯一分解整环，则S的一组元素并不一定有最大公因元。例如在上面的讨论4)中，$S=\mathbf{R}[x^2,x^3]$，取$x^5,x^6\in S$，则其公因元是x^2,x^3及与其相伴的元素，其中并无一元素是所有公因元的倍元，即无最大公因元。

定理3.3 设S为唯一分解的整环，$a_1,a_2,\cdots,a_n\in S$。则存在$a_1,a_2,\cdots,a_n$的最大公因元d，即存在$d\in\mathrm{G.C.D}(a_1,a_2,\cdots,a_n)$。

证明 先证$n=2$的情形。取a_1,a_2的分解式

$$a_1=\delta_1\Big(\prod_i p_i^{n_i}\Big)\Big(\prod_j u_j^{l_j}\Big),$$

$$\alpha_2=\delta_2\left(\prod_i p_i^{m_i}\right)\left(\prod_j v_j^{r_j}\right).$$

经过重新编号以及相伴的不可分解元替换以后，不妨假设，

1）p_i,u_j,v_j皆是不相伴的不可分解元；

2）$n_i>0$，$m_i>0$。

令 $$a_i=\min(n_i,m_i),\qquad d=\prod_i p_i^{a_i}.$$

则不难看出d是α_1,α_2的一个最大公因元。

如$n>2$，我们可以仿照上面的方法写出$\alpha_1,\alpha_2,\cdots,\alpha_n$的分解式，从而直接写出它们的一个最大公因元。我们也可以用数学归纳法，采取的步骤如下：令β为$\alpha_1,\alpha_2,\cdots,\alpha_{n-1}$的最大公因元，则$\beta$与$\alpha_n$的一个最大公因元$d$，必是$\alpha_1,\alpha_2,\cdots,\alpha_n$的一个最大公因元。▌

定义3.12 设S为一整环，α为S的一非零非可逆的元素。如$\alpha|\beta\gamma$时，必有$\alpha|\beta$或$\alpha|\gamma$，则称α为一**素元**。

就像在第一章§2与§5的情形一样，要证明$S[x]$——S是唯一分解的整环——是唯一分解的整环，我们需要证明在$S[x]$中，不可分解元与素元是一物的二名。为此目的，我们先作一些准备工作。

定理3.4 设S为唯一分解的整环，则α是不可分解元$\Longleftrightarrow\alpha$是素元。反之，如在一整环$S$中，每一元素皆可分解为不可分解元的乘积，而且不可分解元与素元是一物的二名，则S是唯一分解的整环。

证明 设S为唯一分解的整环。如α是不可分解元，且有$\alpha|\beta\gamma$，即$\alpha\alpha'=\beta\gamma$。取此式的分解式，

$$\alpha'=\delta'\left(\prod_i u_i^{l_i}\right),$$

$$\beta=\varepsilon_1\left(\prod_i p_i^{n_i}\right),$$

$$\gamma = \varepsilon_2\left(\prod_i q_i^{m_i}\right),$$

$$\alpha\alpha' = \delta'\alpha\prod_i u_i^{l_i} = \varepsilon_1\varepsilon_2\left(\prod_i p_i^{n_i}\right)\prod_i q_i^{m_i}.$$

则知 α 必与 p_i 或 q_i 之一相伴，于是 α 必为 β 或 γ 的因元，所以 α 是素元。

又如 α 是素元时，设 $\alpha=\beta\gamma$。则 $\alpha|\beta\gamma$，于是 $\alpha|\beta$ 或 $\alpha|\gamma$。不妨即令 $\alpha|\beta$。于是

$$\beta = \alpha\delta, \qquad \alpha = \beta\gamma = \alpha(\delta\gamma).$$

因S是整环，故得$\delta\gamma=1$，即γ为可逆元。于是 α 必为不可分解元。

反之，设在整环S中，不可分解元与素元是一物的二名，且每一元素皆可分解成不可分解元的乘积。如有

$$\alpha = \delta\prod_{i=1}^{n} p_i^{m_i} = \varepsilon\prod_{j=1}^{l} q_j^{u_j},$$

则知

$$p_1 | q_1\left(q_1^{u_1-1}\prod_{j=2}^{l} q_j^{u_j}\right).$$

于是

$$p_1|q_1 \quad 或 \quad p_1|q_1^{u_1-1}\prod_{j=2}^{l} q_j^{u_j}.$$

如此反复推导，经过有限次数后，可得一i，使 $p_1|q_i$，即

$$p_1\beta = q_i.$$

因q_i为不可分解元，于是β必为可逆元，即

$$p_1 \overset{a}{\sim} q_i.$$

以$q_i=p_1\beta$代入α的分解式，两边消去p_1后，再用数学归纳法。不难证明，将$q_1, q_2, \cdots, q_l$重新编组后，必有

$$p_i \overset{a}{\sim} q_i, \quad m_i = u_i, \quad n = l,$$

即S是唯一分解的整环。∎

定义3.13 设S是唯一分解的整环。令

$$f(x)=\sum_{i=0}^{n}a_ix^i\in S[x],\quad f(x)\neq 0.$$

多项式$f(x)$的系数$a_0,a_1,\cdots,a_n$的最大公因元的集合$G.C.D(a_0,a_1,\cdots,a_n)$定义为$f(x)$的内涵$C(f(x))$。如果$\deg f(x)\geqslant 1$，且$C(f(x))$等于可逆元的集合，则称$f(x)$为**本原多项式**。

定理3.5(高斯引理) 设S是唯一分解的整环，$f(x)$及$g(x)$是$S[x]$中的非零多项式。则有

$$C(f(x)\cdot g(x))=C(f(x))\cdot C(g(x)).$$

证明 不妨设$f(x),g(x)$的次数不为零。取$d_1\in C(f(x))$，$d_2\in C(g(x))$。令

$$f(x)=d_1f^*(x),\qquad g(x)=d_2g^*(x).$$

则显然$f^*(x)$及$g^*(x)$皆是本原多项式。如能证明$f^*(x)\cdot g^*(x)$也是一本原多项式，则根据$f(x)\cdot g(x)=d_1d_2(f^*(x)\cdot g^*(x))$，即知

$$d_1d_2\in C(f(x)\cdot g(x)).$$

由定义3.11的讨论1)，立得

$$C(f(x))\cdot C(g(x))=C(f(x)\cdot g(x)).$$

以下证明$f^*(x)\cdot g^*(x)$也是一本原多项式。设

$$f^*(x)=a_0+a_1x+\cdots+a_nx^n,$$
$$g^*(x)=b_0+b_1x+\cdots+b_mx^m,$$

其中$a_n\neq 0$，$b_m\neq 0$。假设$f^*(x)\cdot g^*(x)$非本原多项式，取一素元p为其系数的公因元。令i,j为由下式定义的二非负整数：

$$i=\min\{l:\ p\mid a_r,\ \ r=l+1,\cdots,n\},$$
$$j=\min\{l:\ p\mid b_r,\ \ r=l+1,\cdots,m\}.$$

令 $$f^*(x)\cdot g^*(x)=c_0+c_1x+\cdots+c_{n+m}x^{n+m}.$$

则有

$$c_0 = a_0 b_0,$$

$$c_1 = a_0 b_1 + a_1 b_0,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$c_{i+j} = a_i b_j + \sum_{r=i+1}^{i+j} a_r b_{i+j-r} + \sum_{r=j+1}^{i+j} a_{i+j-r} b_r,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$c_{n+m} = a_n b_m.$$

考虑c_{i+j}的展开式。已知

$$p \mid c_{i+j}, \quad p \left| \sum_{r=i+1}^{i+j} a_r b_{i+j-r}, \right.$$

$$p \left| \sum_{r=j+1}^{i+j} a_{i+j-r} b_r. \right.$$

于是推得

$$p \mid a_i b_j, \quad p \mid a_i \text{ 或 } p \mid b_j.$$

这与 i 或 j 的定义相矛盾。由此知道 $f^*(x) \cdot g^*(x)$的系数不可能有素元p为其公因元，也即$f^*(x) \cdot g^*(x)$为一本原多项式。 ▌

定理3.6 设S是唯一分解的整环，则任意非零非可逆的多项式$f(x) \in S[x]$皆可分解成不可分解的多项式的乘积。

证明 设$0 \neq a \in S$。如果$a = g(x)h(x) \in S[x]$，我们考虑其次数，得

$$0 = \deg a = \deg(g(x)h(x)) = \deg g(x) + \deg h(x),$$

于是必有$g(x), h(x) \in S[x]$。由此推知S中的不可分解元也是$S[x]$中的不可分解元。

取 $d \in C(f(x))$。令 $f(x) = df^*(x)$。则d在S中可分解成不可分解元的乘积。根据上段的讨论，d 在$S[x]$中也可分解成不可分解元的乘积。以下求$f^*(x)$的分解式。

如$f^*(x)$为不可分解元，则本定理已证完。如$f^*(x)$可分解成

$$f^*(x)=g(x)h(x),$$

此处$g(x),h(x)$皆不是可逆元。根据定理3.5，

$$C(f^*(x))=C(g(x))C(h(x)),$$

立得$g(x),h(x)$皆是本原多项式。两者皆是不可逆元，必有

$$\deg g(x)\geqslant 1,\qquad \deg h(x)\geqslant 1.$$

于是有

$$\deg g(x)<\deg f^*(x),\qquad \deg h(x)<\deg f^*(x).$$

用数学归纳法，已知$g(x)$及$h(x)$皆可分解成不可分解元的乘积。并乘两者，得 $f^*(x)$也可分解成不可分解元的乘积。∎

定理3.7 设S是唯一分解的整环，则$S[x]$的任意素元必是不可分解元。

证明 设$f(x)\in S[x]$为一素元。如果$f(x)=g(x)h(x)$，则

$$f(x)\mid g(x)h(x),$$

于是$f(x)\mid g(x)$或$f(x)\mid h(x)$。不妨令$f(x)\mid g(x)$，即

$$g(x)=f(x)\delta(x),\qquad f(x)=g(x)h(x)=f(x)\delta(x)h(x).$$

因$S[x]$是整环，$f(x)\neq 0$，自上式的左右两侧消去$f(x)$，得

$$1=\delta(x)h(x).$$

于是$h(x)$是可逆元。由此得知$f(x)$为不可分解元。∎

到此为止，欲证$S[x]$是唯一分解的整环，根据定理3.4，3.6，3.7，仅需证明$S[x]$的不可分解元皆是素元。我们先推广“欧几里得算法”。

定理3.8(欧几里得算法) 设S为一交换环，$f(x)$为$S[x]$中的一非零多项式。令

$$f(x)=a_0+a_1x+\cdots+a_nx^n,\qquad a_n\neq 0.$$

任意给定一次数为m的多项式$g(x)\in S[x]$。令$l=\max\{0,m-n+1\}$，$c=a_n^l$。则必存在$d(x),r(x)\in S[x]$，使

$$cg(x)=d(x)f(x)+r(x),\qquad \deg r(x)<\deg f(x).$$

证明 如$\deg f(x)=n=0$，取$r(x)=0$，$d(x)=a_0^{l-1}g(x)$，即得本定理。以下讨论$\deg f(x)=n>0$的情形。

如 $\deg g(x)<\deg f(x)$，取 $d(x)=0$，$r(x)=cg(x)$，即得本定理。以下我们对 $\deg g(x)$ 用数学归纳法。

令 $f(x),g(x)$ 的展开式如下：

$$f(x)=a_0+a_1x+\cdots+a_nx^n,\qquad a_n\neq0,$$

$$g(x)=b_0+b_1x+\cdots+b_mx^m,\qquad b_m\neq0,$$

此处 $\deg f(x)=n\leqslant\deg g(x)=m$。令

$$h(x)=a_ng(x)-b_mx^{m-n}f(x),$$

不难看出

$$\deg h(x)<\deg g(x).$$

根据数学归纳法，存在 $d'(x)$ 及 $r(x)$，使

$$a_n^{l-1}h(x)=d'(x)f(x)+r(x),\quad \deg r(x)<\deg f(x).$$

于是

$$a_n^lg(x)=a_n^{l-1}(h(x)+b_mx^{m-n}f(x))$$

$$=(d'(x)+b_mx^{m-n})f(x)+r(x).$$ ▌

系 如 S 是域，则在上定理中可取 $c=1$。如此得出的 $d(x)$ 及 $r(x)$ 是由 $g(x)$ 唯一确定的。

证明 如 S 是域，则非零元素 c 是可逆的。在原式

$$cg(x)=d(x)f(x)+r(x),\qquad \deg r(x)<\deg f(x)$$

两边乘以 c^{-1}，即得

$$g(x)=(c^{-1}d(x))f(x)+(c^{-1}r(x)),\ \deg(c^{-1}r(x))<\deg f(x).$$

本系的第二部分证法如下：如有

$$g(x)=d(x)f(x)+r(x),\qquad \deg r(x)<\deg f(x),$$

$$g(x)=d'(x)f(x)+r'(x),\qquad \deg r'(x)<\deg f(x),$$

则有

$$(d(x)-d'(x))f(x)=r'(x)-r(x).$$

如 $d(x)-d'(x)\neq0$，比较上式两边的次数，得

$$\deg(r'(x)-r(x))=\deg(d(x)-d'(x))+\deg f(x)$$

$$\geqslant\deg f(x)>\deg(r'(x)-r(x)).$$

此是一矛盾，故知 $d(x)-d'(x)=0$，于是必有 $r'(x)-r(x)=0$。▌

定理3.9 设 K 是域。$f_1(x),f_2(x)\in K[x]$。令

$$(f_1(x),f_2(x))$$
$$=\{a_1(x)f_1(x)+a_2(x)f_2(x):\ a_1(x),a_2(x)\in K[x]\}.$$
则存在$f(x)$，使
$$(f_1(x),f_2(x))=(f(x))=\{a(x)f(x):\ a(x)\in K[x]\},$$
而且$f(x)$是 $f_1(x),f_2(x)$的最大公因元。

证明 如 $f_1(x)=0$，显然有 $(f_1(x),f_2(x))=(f_2(x))$。如 $f_1(x)\neq 0$，取 $f(x)$为 $(f_1(x),f_2(x))$ 中次数最小的非零元素。根据定理3.8的系，存在 $d_1(x),r_1(x),d_2(x),r_2(x)$，使
$$f_1(x)=d_1(x)f(x)+r_1(x),\qquad \deg r_1(x)<\deg f(x);$$
$$f_2(x)=d_2(x)f(x)+r_2(x),\qquad \deg r_2(x)<\deg f(x).$$
移项后不难看出，$r_1(x),r_2(x)$皆在$(f_1(x),f_2(x))$中。根据 $f(x)$ 的选法，立得$r_1(x)=r_2(x)=0$。于是
$$a_1(x)f_1(x)+a_2(x)f_2(x)$$
$$=(a_1(x)d_1(x)+a_2(x)d_2(x))f(x)\in(f(x)).$$
反之，已知 $f(x)\in(f_1(x),f_2(x))$，即
$$f(x)=\beta_1(x)f_1(x)+\beta_2(x)f_2(x),$$
于是
$$a(x)f(x)=a(x)\beta_1(x)f_1(x)$$
$$+a(x)\beta_2(x)f_2(x)\in(f_1(x),f_2(x)).$$
故$(f(x))=(f_1(x),f_2(x))$。读者自证 $f(x)$是 $f_1(x)$及 $f_2(x)$的最大公因元。▌

系 设K是域，$f_1(x),f_2(x),\cdots,f_n(x)\in K[x]$。令
$$(f_1(x),f_2(x),\cdots,f_n(x))=\left\{\sum_i a_i(x)f_i(x):\ a_i(x)\in K[x]\right\}.$$
则存在$f(x)$，使
$$(f_1(x),f_2(x),\cdots,f_n(x))=(f(x)),$$
而且$f(x)$是 $f_1(x),f_2(x),\cdots,f_n(x)$的最大公因元。

定理3.10 设K是域，则 $K[x]$的不可分解元皆是素元。

证明 令 $f(x)$为一不可分解元，$f(x)\mid g(x)h(x)$。根据定理3.9，得出

$$(f(x),g(x))=(l(x)).$$

$l(x)$或为可逆元，或为不可逆元。如$l(x)$为可逆元，则根据定义3.9的讨论5)，知$l(x)\in K^*=K\backslash\{0\}$。于是令$l=l(x)$，有

$$l=\alpha(x)f(x)+\beta(x)g(x).$$

乘以$l^{-1}h(x)$，得

$$h(x)=l^{-1}\alpha(x)f(x)h(x)+l^{-1}\beta(x)g(x)h(x).$$

显然，$f(x)$是上式右侧的因元，于是有$f(x)|h(x)$。如$l(x)$为不可逆元。因为

$$f(x)=1\times f(x)+0\times g(x)\in(f(x),g(x))=(l(x)),$$

故有

$$f(x)=a(x)l(x)\quad(\text{同理}g(x)=\beta(x)l(x)).$$

已知$f(x)$为不可分解元，$l(x)$为不可逆元，于是$a(x)$必为可逆元，即$a(x)=a\in K^*=K\backslash\{0\}$。由此得

$$l(x)=a^{-1}f(x),\qquad g(x)=a^{-1}\beta(x)f(x).$$

即$f(x)|g(x)$。如此已证$f(x)|h(x)$或$f(x)|g(x)$，即$f(x)$为一素元。▎

定理3.11 设K是域，则$K[x]$是唯一分解的整环。

证明 综合定理3.4，3.6，3.7，3.10，立得本定理。▎

以下我们要应用上定理去解决广义的问题。

定理3.12 设S是唯一分解的整环，K为其比域。一本原多项式$f(x)\in S[x]$在$S[x]$中为不可分解元的充要条件是$f(x)$在$K[x]$中为不可分解元。

证明 设$f(x)$在$K[x]$中可分解为

$$f(x)=\alpha(x)\beta(x),\qquad \deg\alpha(x)\geqslant1,\ \deg\beta(x)\geqslant1.$$

因为$\alpha(x),\beta(x)$的系数在比域K中，皆形如$a/b(a,b\in S)$，故取$\alpha(x)$的系数的公分母d_1及$\beta(x)$的系数的公分母d_2，则有$d_1\alpha(x)$，$d_2\beta(x)\in S[x]$。令$\alpha^*(x),\beta^*(x)$为本原多项式，使下式成立：

$$d_1\alpha(x)=e_1\alpha^*(x),\qquad d_2\beta(x)=e_2\beta^*(x),\qquad e_1,e_2\in S.$$

则将$f(x)$的分解式乘以d_1d_2后，得

$$d_1 d_2 f(x) = d_1\alpha(x) d_2\beta(x) = e_1\alpha^*(x) e_2\beta^*(x)$$
$$= e_1 e_2 \alpha^*(x)\beta^*(x).$$

应用高斯引理，在上式两侧取内涵，得出

$$d_1 d_2 \mid e_1 e_2, \qquad \frac{e_1 e_2}{d_1 d_2} \in S.$$

于是

$$f(x) = \frac{e_1 e_2}{d_1 d_2}\alpha^*(x)\beta^*(x),$$

即 $f(x)$在$S[x]$中可以分解。

反之，若 $f(x)$在 $S[x]$ 中可分解为不可逆元 $g(x), h(x)$ 的乘积，因为$f(x)$为本原多项式，所以

$$\deg g(x) \geqslant 1, \qquad \deg h(x) \geqslant 1.$$

于是$g(x), h(x)$在$K[x]$中也为不可逆元。因此$f(x) = g(x)h(x)$也是 $f(x)$在 $K[x]$中的分解式。 ▌

定理3.13 如S为唯一分解的整环，则$S[x]$中的不可分解元皆是素元。

证明 任取$S[x]$中的一个不可分解元$f(x)$。

1) 先证如$f(x) = f \in S$，则f必为S的不可分解元，即是S中的素元。为什么呢？假如$f = \alpha\beta$，α, β是S的不可逆元。因$f(x) = f$是$S[x]$中的不可分解元，于是α, β两者之一——不妨即令为α——必为$S[x]$的可逆元，即存在$\gamma(x)$，使

$$\alpha \cdot \gamma(x) = 1.$$

讨论上式两边的次数后，立得

$$\deg \gamma(x) = 0, \qquad \gamma(x) \in S,$$

也即α是S的可逆元。此是一矛盾。

2) 如$f(x) = f \in S$。设$f \mid g(x)h(x)$。令

$$g(x) = d_1 g^*(x), \qquad h(x) = d_2 h^*(x),$$
$$f \cdot l(x) = g(x)h(x), \qquad l(x) = d_3 l^*(x),$$

其中$g^*(x), h^*(x), l^*(x)$是本原多项式。根据高斯引理，得

$$C(f)C(l(x)) = C(f \cdot l(x)) = C(g(x)h(x))$$
$$= C(g(x))C(h(x)).$$

于是有

$$fd_3 \sim d_1 d_2,$$

即有一可逆元 δ，使

$$\delta f d_3 = d_1 d_2, \qquad f \mid d_1 d_2.$$

根据 1)，f 是 S 的素元，于是有

$$f \mid d_1 \quad 或 \quad f \mid d_2.$$

由此得 $f \mid g(x)$ 或 $f \mid h(x)$。

3) 如 $f(x) \overline{\in} S$。令 K 为 S 的比域。根据定理 3.12，$f(x)$ 是 $K[x]$ 中的不可分解元。又根据定理 3.10，得知 $f(x)$ 是 $K[x]$ 的素元。

以下我们要证明 $f(x)$ 是 $S[x]$ 的素元。设在 $S[x]$ 中，$f(x)$ 是 $g(x) \cdot h(x)$ 的因元，即 $f(x) \mid g(x)h(x)$。于是有 $l(x) \in S[x]$，使

$$l(x)f(x) = g(x)h(x).$$

在 $K[x]$ 中考虑上式，因 $f(x)$ 是 $K[x]$ 的素元，所以

$$f(x) \mid g(x) \quad 或 \quad f(x) \mid h(x).$$

不妨即令 $f(x) \mid g(x)$。于是有 $r(x) \in K[x]$，使下式成立：

$$r(x)f(x) = g(x).$$

取 d 为 $r(x)$ 的系数的公分母，以 d 乘上式，得

$$(d \cdot r(x))f(x) = d \cdot g(x).$$

令 $r^*(x)$ 为一本原多项式，使下式成立：

$$d \cdot r(x) = e \cdot r^*(x), \qquad e \in S.$$

请读者注意，$f(x)$ 也必是本原多项式（否则 $f(x)$ 可分解）。由

$$(d \cdot r(x))f(x) = e(r^*(x)f(x)) = d \cdot g(x),$$

应用高斯引理，得

$$e \in C(d \cdot g(x)).$$

显然，d 是多项式 $dg(x)$ 的系数的公因元，于是有

$$d \mid e, \quad \frac{e}{d} r^*(x) \in S[x].$$

从 $g(x)=\left(\frac{e}{d}r^*(x)\right)f(x)$，得出在$S[x]$中，$f(x)|g(x)$。

综上所述，我们证明了$f(x)$是$S[x]$中的素元。▎

定理3.14 如果S是唯一分解的整环，则$S[x]$是唯一分解的整环。

证明 易于自定理3.4，3.6，3.7，3.13导出。▎

系 1 如果S是唯一分解的整环，则$S[x_1,x_2,\cdots,x_n]$是唯一分解的整环。

系 2 如果K是域，则$K[x_1,x_2,\cdots,x_n]$是唯一分解的整环。

习　题

1．试求$x^6+2x^4+2x^3+x^2+2x+1$与$x^5+2x^3+x^2+x+1$的最大公因子。

2．试求x^m-1与x^n-1的最大公因子。

3．设$a_1,a_2,\cdots,a_n$为互不相同的正整数，证明

$$f(x)=\prod_{i=1}^{n}(x-a_i)^2+1$$

在$Q[x]$内不可约(不可分解)。

4．在$Z_6[x]$内取多项式：

$$f(x)=2x^5-3x^2+1,\qquad g(x)=2x^6+x-1.$$

试求$d(x),r(x)\in Z_6[x]$，使

$$2^2g(x)=d(x)f(x)+r(x),\qquad \deg r(x)<\deg f(x).$$

5．证明$f(x)=x^3+x^2+1$是$Z_2[x]$的素元。

6．在$Z_5[x]$内求$f(x)=x^5-3x^3+3x^2+4x+2$的素因子分解式。

7．任取次数$\geqslant 1$的首一多项式$f(x)\in Z[x]\subseteq Q[x]$。证明$f(x)$在$Q[x]$中可以分解$\Longrightarrow f(x)$看作$Z_p[x]$内的多项式也可以分解，其中$p$为一素数。

8．证明：整系数多项式$f(x)$，$g(x)$在有理数域上互素的充要条件是，除有限多个素数外，对其他任一素数p，$f(x)$与$g(x)$在$\mathbf{Z}_p[x]$内互素。

9．求$\mathbf{Z}_3[x]$内所有首项系数为1的不可约三次多项式。

10．证明$f(x)=x^4-10x^2+1$在$\mathbf{Q}[x]$内不可约，但对任一素数p，$f(x)$在$\mathbf{Z}_p[x]$内可约。

11．举出一个整系数多项式$f(x)$，它在$\mathbf{Q}[x]$内可约，但存在一个素数p，使$f(x)$在$\mathbf{Z}_p[x]$内不可约。

12．设S是唯一分解整环，$f(x)$是$S[x]$内首一多项式，F是S的比域。若$g(x)$是$f(x)$在$F[x]$内的一个首一因子，证明：$g(x)\in S[x]$。

13．证明$(x^2+x+1)\mid(x^{3m}+x^{3n+1}+x^{3p+2})$（$m,n,p$为正整数）。

14．设R是交换环，证明：$f(x)=\sum_{i=0}^{n}a_ix^i\in R[x]$是一个可逆元$\Leftrightarrow a_0$是可逆元及$a_i(i\geqslant1)$是幂零元，即存在$m_i$，使

$$a_i^{m_i}=0\quad(i=1,2,\cdots,n).$$

15．设$f(x)=x^p-x+a\in\mathbf{Z}_p[x]$，此处$p$是一素数。证明

$$f(x)\text{可约}\Leftrightarrow a=0.$$

16．证明$x^{89}+89x^{88}+178x^{50}-90x+11$不可约（在$\mathbf{Q}[x]$内）。

17．设R是一个交换环，$f(x)\in R[x]$是一个零因子，证明：存在$a\in R$，$a\neq0$，使$af(x)=0$。

18．证明x^6+x^3+1在$\mathbf{Q}[x]$内不可约。

19．$g(x)$-adic进位法．与整数的十进位法类似，在多项式环内我们有$g(x)$-adic进位法如下：设$\deg g(x)\geqslant1$．任取$f(x)\in k[x]$，此处k是一个域．证明存在唯一的$f_0(x),\cdots,f_r(x)\in k[x]$，使

$$f(x)=\sum_i f_i(x)(g(x))^i,$$

其中$\deg f_i(x) < \deg g(x)$。

20. 证明 $x^2+y^2-x^3$在 $\mathbf{Q}[x,y]$内不可约。

21. 在 $\mathbf{C}[x,y,z]$内分解多项式

$-x^3-y^3-z^3+x^2(y+z)+y^2(x+z)+z^2(x+y)-2xyz$。

22. 将$x^3+y^3+z^3-3xyz$分别在$\mathbf{Z}[x,y,z]$和$\mathbf{C}[x,y,z]$内进行因式分解。

§4 对称式，结式及判别式

设R为一交换环，$R[x]$为其多项式环。令$f(x)\in R[x]$，$b\in R$，我们定义$f(x)=\sum_i a_i x^i$在$x=b$的值为$f(b)=\sum_i a_i b^i$。如$f(b)=0$，则称$x=b$是$f(x)$的根。根也称为零点。我们可以推广以上的定义到多元多项式环$R[x_1,x_2,\cdots,x_n]$。令

$$f(x_1,x_2,\cdots,x_n)$$

$$=\sum a_{i_1 i_2\cdots i_n} x_1^{i_1} x_2^{i_2}\cdots x_n^{i_n}\in R[x_1,x_2,\cdots,x_n],$$

$(b_1,b_2,\cdots,b_n)\in R\times R\times\cdots\times R$。我们定义$f(x_1,x_2,\cdots,x_n)$在

$$(x_1,x_2,\cdots,x_n)=(b_1,b_2,\cdots,b_n)$$

的值为

$$f(b_1,b_2,\cdots,b_n)=\sum a_{i_1 i_2\cdots i_n} b_1^{i_1} b_2^{i_2}\cdots b_n^{i_n}.$$

如 $f(b_1,b_2,\cdots,b_n)=0$，则称

$$(x_1,x_2,\cdots,x_n)=(b_1,b_2,\cdots,b_n)$$

是$f(x_1,x_2,\cdots,x_n)$的零点。

定理3.15 设R为交换环，$R[x]$为其多项式环，$f(x)\in R[x]$。则$x=b$是$f(x)$的根的充要条件是$(x-b)\mid f(x)$，即

$$f(x)\in((x-b))=\{g(x)(x-b):\ g(x)\in R[x]\}.$$

证明 读者自证。▎

系 1 如R是整环，$f(x)\in R[x]$，$\deg f(x)=n$，则$f(x)$最多

只有 n 个不同的根。

证明 令K是R的比域，则$K[x]$是唯一分解整环。而 $f(x)\in R[x]\subset K[x]$，于是$f(x)$在$K[x]$中的分解式

$$f(x)=\delta\prod_i p_i(x)^{m_i}$$

最多只有 n 个一次式，即$f(x)$在K中最多只有 n 个不同的根。于是 $f(x)$在R中最多只有 n 个不同的根。

系 2 如 R 是域，$f(x)\in R[x]$，$\deg f(x)=n$，则 $f(x)$最多只有 n 个不同的根。 ▎

讨论 1) 如果R是一非整环的交换环，则一多项式可能有多于其次数的根。例如，取 $R=\boldsymbol{Z}_8$，令 $f(x)=x^3$，则 $x=[0]_8$，$[2]_8$，$[4]_8$，$[6]_8$皆是 $f(x)$的根。

2) 如果$(x-b)^2|f(x)$，则称$x=b$是$f(x)$的**重根**。 ▎

一个多项式$f(x)$的根与$f(x)$的系数的关系，是一饶有趣味的数学题材。我们用“变数法”——令其根为变数$x_1,x_2,\cdots,x_n$——来阐明这个关系。

在多元多项式环$R[x_1,x_2,\cdots,x_n,y]$中，取如下之多项式：

$$\begin{aligned}F(x_1,x_2,\cdots,x_n,y)&=\prod_{i=1}^{n}(y-x_i)\\&=y^n-a_1(x_1,x_2,\cdots,x_n)y^{n-1}+a_2(x_1,x_2,\cdots,x_n)y^{n-2}-\cdots\\&\quad+(-1)^n a_n(x_1,x_2,\cdots,x_n),\end{aligned}$$

其中

$$\begin{aligned}&a_1(x_1,\cdots,x_n)=x_1+x_2+\cdots+x_n,\\&a_2(x_1,\cdots,x_n)=x_1x_2+x_1x_3+x_1x_n+x_2x_3+\cdots+x_{n-1}x_n,\\&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\&a_{n-1}(x_1,\cdots,x_n)=x_1x_2\cdots x_{n-1}+x_1x_3\cdots x_n+\cdots+x_2x_3\cdots x_n,\\&a_n(x_1,\cdots,x_n)=x_1x_2\cdots x_n.\end{aligned}$$

它们称为 $x_1,x_2,\cdots,x_n$ 的**初等对称多项式**。

一般言之，如果 $g(x_1,x_2,\cdots,x_n)(\in R[x_1,x_2,\cdots,x_n])$ 在任意调换 $x_1,x_2,\cdots,x_n$ 后仍然不变，则称之为一**对称多项式**。很显然，如把 $F(x_1,x_2,\cdots,x_n,y)$ 中的变数 $x_1,x_2,\cdots,x_n$ 任意加以调换，则此多项式仍然不变。于是其以 y 为变数展开后的系数 $a_1,a_2,\cdots,a_n$ 必然皆是对称多项式。

对于初等对称多项式 $a_1,a_2,\cdots,a_n$ 可以引入比重的概念。令 a_1 的比重为 $1,\cdots,a_i$ 的比重为 $i,\cdots,a_n$ 的比重为 n。令

$$\prod_i a_i^{j_i}$$

的比重为 $\sum i j_i$。令

$$g(a_1,a_2,\cdots,a_n)=\sum a_{j_1j_2\cdots j_n}\prod a_i^{j_i}$$

的比重为 $\max\left\{\sum i\, j_i:\, a_{j_1j_2\cdots j_n}\neq 0\right\}$，即单项的最大比重。我们有如下的定理。

定理3.16（牛顿定理） 设 $f(x_1,x_2,\cdots,x_n)\in R[x_1,x_2,\cdots,x_n]$ 为一 m 次对称多项式。则存在一个比重为 m 的 n 元多项式 $g(a_1,a_2,\cdots,a_n)$，使

$$f(x_1,x_2,\cdots,x_n)=g(a_1,a_2,\cdots,a_n).$$

即 $f(x_1,x_2,\cdots,x_n)\in R[a_1,a_2,\cdots,a_n]\subset R[x_1,x_2,\cdots,x_n]$。

证明 我们对变数的个数 n 及次数 m 作双重归纳。如 $n=1$，则 $a_1=x_1$，本定理是显然的。设 $n>1$，并且对于少于 n 个的变数，本定理皆成立。以下证明 n 个变数的情形。

当 $m=0$ 时，则 $f(x_1,\cdots,x_n)\in R$，本定理也是显然的。我们设 $m>0$，并且对于小于 m 次的对称多项式，本定理也皆成立。以下再证明次数为 m 的情形。

令

$$a_i'(x_1,\cdots,x_{n-1})=a_i(x_1,\cdots,x_{n-1},0),\qquad i=1,\cdots,n-1.$$

不难看出，$a_1',\cdots,a_{n-1}'$ 即是变数 $x_1,\cdots,x_{n-1}$ 的初等对称多项式。

又考虑 $f(x_1,\cdots,x_{n-1},0)$。不难看出，这是 $x_1,\cdots,x_{n-1}$ 的对称多项式，且

$$\deg_{x_1,\cdots,x_{n-1}}(f(x_1,\cdots,x_{n-1},0)) \leqslant \deg_{x_1,\cdots,x_n}(f(x_1,\cdots,x_n)) = m。$$

于是，根据归纳法，存在$g'(a'_1,\cdots,a'_{n-1})$，使下列各式成立：

1) $g'(a'_1,\cdots,a'_{n-1}) = f(x_1,\cdots,x_{n-1},0)$；

2) $g'(a'_1,\cdots,a'_{n-1})$的比重$\leqslant m$；

令

$$h(x_1,\cdots,x_n) = f(x_1,\cdots,x_n) - g'(a_1,\cdots,a_{n-1}),$$

立得

3) $h(x_1,\cdots,x_n)$是$x_1,\cdots,x_n$ 的对称多项式；

4) $g'(a_1,\cdots,a_{n-1})$的比重$\leqslant m$；

5) $\deg_{x_1,\cdots,x_n} g'(a_1,\cdots,a_{n-1}) \leqslant m = \deg_{x_1,\cdots,x_n} f(x_1,\cdots,x_n)$；

于是有

6) $\deg_{x_1,\cdots,x_n} h(x_1,\cdots,x_n) \leqslant m$；

但

7) $h(x_1,\cdots,x_{n-1},0) = f(x_1,\cdots,x_{n-1},0) - g'(a'_1,\cdots,a'_{n-1}) = 0$，

根据定理3.15，我们得出$x_n | h(x_1,\cdots,x_n)$，即在$h(x_1,\cdots,x_n)$的展开式

$$h(x_1,\cdots,x_n) = \sum b_{j_1\cdots j_n} x_1^{j_1}\cdots x_n^{j_n}$$

中每一单项皆为 x_n 整除。因为$h(x_1,\cdots,x_n)$是对称多项式，经过x_i与x_n对换后，得出$x_i | h(x_1,\cdots,x_n)$。于是在$h(x_1,\cdots,x_n)$的展开式中，其每一单项皆被 $x_1,\cdots,x_n$ 整除，故每一单项皆被$\prod_{i=1}^{n} x_i$整除，也即

$$\prod_{i=1}^{n} x_i \Big| h(x_1,\cdots,x_n).$$

令

$$h(x_1,\cdots,x_n)=\left(\prod_{i=1}^{n}x_i\right)h'(x_1,\cdots,x_n)=a_nh'(x_1,\cdots,x_n).$$

则有

8) $h'(x_1,\cdots,x_n)$是对称多项式;

9) $\deg_{x_1,\cdots,x_n}h'(x_1,\cdots,x_n)\leqslant m-n$.

根据数学归纳法，$h'(x_1,\cdots,x_n)=g''(a_1,\cdots,a_n)$，而且$g''(a_1,\cdots,a_n)$的比重$\leqslant m-n$. 于是

$$f(x_1,\cdots,x_n)=g'(a_1,\cdots,a_n)+a_ng''(a_1,\cdots,a_n)=g(a_1,\cdots,a_n).$$

不难看出，$g(a_1,\cdots,a_n)$的比重$\leqslant m$. 我们仅须证明其比重是m.
易见

$$\deg_{x_1,\cdots,x_n}g(a_1,\cdots,a_n)\leqslant g(a_1,\cdots,a_n)\text{的比重},$$

而上式左侧即是$f(x_1,\cdots,x_n)$的次数m，于是$g(a_1,\cdots,a_n)$的比重必为m. ▎

讨论 在上面的定理中，"对称"是指对群S_n对称，即，令ρ为S_n中的任意元素，定义

$$\rho(f(x_1,\cdots,x_n))=f(x_{\rho(1)},\cdots,x_{\rho(n)}).$$

多项式$f(x_1,\cdots,x_n)$是对称的，意即对S_n的任意元素ρ而言，下式恒成立:

$$\rho(f(x_1,\cdots,x_n))=f(x_1,x_2,\cdots,x_n).$$

这种对称也可称为S_n对称。如取S_n的一个子群G，我们也可以如法定义G对称。一般言之，只要G作用在$R[x_1,\cdots,x_n]$上，即可定义G对称。在这一类的群G的作用下，上面的牛顿定理不能简单地推广了。对这一方面的研究，现在还在继续开展中。▎

设K为一域。任取二多项式$f(y),g(y)\in K[y]$. 在什么条件下，$f(y)$与$g(y)$有一次数大于零的公因元呢？如果在整数环$\boldsymbol{Z}$中考虑类似的问题，一般反复用"欧几里得算法"——即长除法——便可求出其公因数了。在一元多项式环中，除了应用同法之外，尚有一更系统的方法，直接写出二多项式$f(y),g(y)$有次数大于

零的公因元的充要条件。此一方法即下面要谈的“结式”方法。

令$f(y)$及$g(y)$可写成下列的展开式：

$$f(y)=a_0+a_1y+a_2y^2+\cdots+a_ny^n,$$
$$g(y)=b_0+b_1y+b_2y^2+\cdots+b_my^m,$$

其中$a_n\neq 0$，而b_m可以为零。令$h(y)$为其公因元，且$\deg h(y)\geqslant 1$。于是有

$$f(y)=\alpha(y)h(y),\qquad -g(y)=\beta(y)h(y).$$

$\beta(y)f(y)+\alpha(y)g(y)=0$，$\deg\alpha(y)<n$，$\deg\beta(y)<\deg g(y)$。我们用“不定系数法”继续讨论。设$u_1,\cdots,u_n,v_1,\cdots,v_m$为变数，令

$$A(y)=u_1+u_2y+\cdots+u_ny^{n-1},$$
$$B(y)=v_1+v_2y+\cdots+v_my^{m-1}.$$

则适当取$u_1,\cdots,u_n,v_1,\cdots,v_m$的值以后，$A(y)$即成$\alpha(y)$，$B(y)$即成$\beta(y)$。换言之，在下列方程式中，

$$B(y)f(y)+A(y)g(y)=0,$$

$u_1,\cdots,u_n,v_1,\cdots,v_m$可取一组不全为零的值，使方程式对变数$y$而言，其系数全为零。如按照$y^{n+m-1},y^{n+m-2},\cdots,y,1$的系数排出，则得下列一组联立多元一次方程式：

$$\begin{array}{lll}
y^{n+m-1}: & a_nv_m \qquad\qquad + b_mu_n & =0,\\
y^{n+m-2}: & a_{n-1}v_m+a_nv_{m-1} \qquad + b_{m-1}u_n+b_mu_{n-1} & =0,\\
\cdots\cdots & \cdots\cdots\cdots\cdots\cdots\cdots & \\
y^{m-1}: & a_0v_m+a_1v_{m-1}+\cdots+b_{m-n}u_n+b_{m-n+1}u_{n-1} & \\
 & \qquad\qquad +\cdots & =0,\\
y^{m-2}: & \qquad a_0v_{m-1}+\cdots\cdots\cdots\cdots & =0,\\
\cdots\cdots & \cdots\cdots\cdots\cdots\cdots\cdots & \\
1: & \qquad\qquad a_0v_1 \qquad +b_0u_1 & =0.
\end{array}$$

此方程组有不全为零的公解的充要条件，是其系数矩阵的行列式为零。关于此一充要条件，如K是常见的$\boldsymbol{Q}$，$\boldsymbol{R}$或$\boldsymbol{C}$时，[3]读者应已耳熟能详了。至于K是一般域的情形，这一充要条件的证法，

与K为实数域$\mathbf{R}$时，完全相同，读者试自证之。如果读者不能证明此点，则应令$K=\mathbf{Q},\mathbf{R}$或$\mathbf{C}$，以了解本节。

我们把联立方程组的系数排成矩阵，然后把行与列互相调换，称其行列式为$f(y)$与$g(y)$的结式，记为$\mathrm{Res}_y(f(y),g(y))$。即

$$\mathrm{Res}_y(f(y),g(y))$$

$$=\det\begin{pmatrix} a_n & a_{n-1} & \cdots & a_0 & 0 & 0 & \cdots & 0 \\ 0 & a_n & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ & & \cdots & \cdots & \cdots & \cdots & & \\ & & & \cdots & \cdots & \cdots & \cdots & \\ 0 & 0 & \cdots & \cdots & a_n & a_{n-1} & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & \cdots & b_1 & b_0 & \cdots & 0 \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0 & \cdots & b_m & b_{m-1} & \cdots & \cdots & \cdots & b_0 \end{pmatrix}\begin{matrix} \left.\right\} m\text{行} \\ \left.\right\} n\text{行} \end{matrix}.$$

于是我们有下列关于结式的定理。

定理3.17 设K为域，$f(y),g(y)\in K[y]$。又令

$$f(y)=a_0+a_1y+\cdots+a_ny^n,$$

$$g(y)=b_0+b_1y+\cdots\cdots+b_my^m,$$

则$\mathrm{Res}_y(f(y),g(y))=0 \Longleftrightarrow a_n=0=b_m$或$f(y),g(y)$有一次数$\geqslant 1$的公因元。

证明 $\Longleftarrow$。如果$a_n=0=b_m$，则$\mathrm{Res}_y(f(y),g(y))$的第一列皆为零，于是$\mathrm{Res}_y(f(y),g(y))$自然为零。如果$a_n,b_m$两者之间有一个非零，则不妨设$a_n\neq0$，证明已见上文。

$\Longrightarrow$。如$a_n=0=b_m$，则无甚可证。如a_n，b_m两者之间有一个非零，则不妨假设$a_n\neq0$。我们应用上文的符号，于是可求出一组$u_1,\cdots,u_n,v_1,\cdots,v_m$的不全为零的值。代入$A(y)$及$B(y)$中，令所得的多项式为$\alpha(y),\beta(y)\in K[y]$。于是有

$$\beta(y)f(y)+\alpha(y)g(y)=0,$$

其中$\deg\alpha(y)<\deg f(y)=n$。如果$f(y),g(y)$无不可逆的公因元，

则有$(f(y),g(y))=(1)$。即存在$\delta(y),\varepsilon(y)\in K[y]$，使

$$1=\delta(y)f(y)+\varepsilon(y)g(y).$$

乘以$\alpha(y)$，得出

$$\begin{aligned}\alpha(y)&=\alpha(y)\delta(y)f(y)+\varepsilon(y)\alpha(y)g(y)\\&=(\alpha(y)\delta(y)-\beta(y)\varepsilon(y))f(y).\end{aligned}$$

考察上式两边的次数，必得$\alpha(y)=0$。于是

$$\beta(y)f(y)=-\alpha(y)g(y)=0,$$

即$\beta(y)=0$。换言之，$u_1,\cdots,u_n,v_1,\cdots,v_m$的值全为零。这是一矛盾。▌

以下我们欲求出结式$\mathrm{Res}_y(f(y),g(y))$与$f(y),g(y)$的根的关系。我们用“变数法”来处理这个问题。为简便起见，令$a_n=b_m=1$，$f(y),g(y)$如下式：

$$f(y)=\prod_{i=1}^{n}(y-x_i)=\sum_{i=0}^{n}a_iy^i,$$

$$g(y)=\prod_{j=1}^{m}(y-z_j)=\sum_{i=0}^{m}b_iy^i.$$

此处$x_1,\cdots,x_n,y,z_1,\cdots,z_m$皆是变数。于是

$$a_i=(-1)^{n-i}\sigma_{n-i},\quad b_j=(-1)^{m-j}\rho_{m-j},$$

其中σ_{n-i}及ρ_{m-j}是$x_1,\cdots,x_n$及$z_1,\cdots,z_m$的初等对称多项式。在下列结式中，如果第一行乘以x_1，第i（$i\leqslant m$）行乘以x_1^i，第j（$j>m$）行乘以x_1^{j-m}，…，第$(n+m)$行乘以x_1^n，即如下式

$$(1)\qquad\begin{bmatrix}1&a_{n-1}&\cdots&a_0&0&0&\cdots&0\\0&1&\cdots&a_1&a_0&0&\cdots&0\\&&\cdots&\cdots&\cdots&\cdots&&\\&&&\cdots&\cdots&\cdots&\cdots&\\0&0&\cdots&\cdots&1&a_{n-1}&\cdots&a_0\\1&b_{m-1}&\cdots&\cdots&b_1&b_0&\cdots&0\\&\cdots&\cdots&\cdots&\cdots&\cdots&\cdots&\\0&\cdots&1&b_{m-1}&\cdots&\cdots&\cdots&b_0\end{bmatrix}\begin{matrix}\times x_1\\\times x_1^2\\\vdots\\\vdots\\\times x_1^m\\\times x_1\\\vdots\\\times x_1^n\end{matrix}$$

则对变数 $x_1,\cdots,x_n,z_1,\cdots,z_m$ 而言，各列都是齐次式，即第一列是一次式，…，第 i 列是 i 次式，…，第$(n+m)$列是$(n+m)$次式。展开行列式时，由于展开式中任一项都是从每一列中取一项做乘积，于是得出，原来的结式是 $x_1,\cdots,x_n,z_1,\cdots,z_m$ 的齐次式，而其次数为

$$\begin{aligned}
&1+2+\cdots+(m+n)-(1+2+\cdots+n)-(1+2+\cdots+m)\\
&=\frac{1}{2}(m+n)(m+n+1)-\frac{1}{2}n(n+1)-\frac{1}{2}m(m+1)\\
&=mn.
\end{aligned}$$

我们将证明如下的定理。

定理3.18 用上面的记号，我们有

$$\begin{aligned}
\operatorname{Res}_y(f(y),g(y))&=\prod_{i,j}(x_i-z_j)=\prod_i g(x_i)\\
&=(-1)^{nm}\prod_j f(z_j).
\end{aligned}$$

证明 我们分三个步骤来证明本定理。

1）$\operatorname{Res}_y(f(y),g(y))$是 x_i,z_j的次数为 mn 的齐次式，证明见上文。

2）$\prod_{i,j}(x_i-z_j)=\prod_i g(x_i)\,\Big|\,\operatorname{Res}_y(f(y),g(y))$.

显然，在$K[x_1,\cdots,x_n,z_1,\cdots,z_m]$中，如果 $i\neq l$，则

$$g(x_i)=\prod_j(x_i-z_j)\quad 与\quad g(x_l)=\prod_j(x_l-z_j)$$

没有不可逆的公因元。所以仅须证明，对任意的 i，我们恒有

$$g(x_i)\,|\,\operatorname{Res}_y(f(y),g(y)).$$

在上文的结式(1)中，第一列乘以 x_i^{m+n}，然后把第 l 列与 $x_i^{m+n-l+1}$的乘积加到第一列上，此处 l 取尽 $2,3,\cdots,m$。则所得的第一列成为

$$\begin{vmatrix} x_i^m f(x_i) \\ x_i^{m-1} f(x_i) \\ \vdots \\ x_i f(x_i) \\ x_i^n g(x_i) \\ x_i^{n-1} g(x_i) \\ \vdots \\ x_i g(x_i) \end{vmatrix} = \begin{vmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ x_i^n g(x_i) \\ x_i^{n-1} g(x_i) \\ \vdots \\ x_i g(x_i) \end{vmatrix} .$$

从第一列中取出公因元$g(x_i)$，立得

$$g(x_i) \mid x_i^{n+m} \mathrm{Res}_y(f(y), g(y)).$$

显然，$g(x_i)=\prod\limits_{j}(x_i-z_j)$与$x_i^{n+m}$之间无不可逆的公因元。于是必有

$$g(x_i) \mid \mathrm{Res}_y(f(y), g(y)).$$

3）显然，$\prod\limits_{i,j}(x_i-z_j)$的次数是$mn=\mathrm{Res}_y(f(y), g(y))$的次数，于是立得

$$\mathrm{Res}_y(f(y), g(y)) = c\prod_{i,j}(x_i-z_j),$$

其中$c\in K$。以下我们证明$c=1$。

令　$x_1=x_2=\cdots=x_n=0$，$z_1=z_2=\cdots=z_m=1$，则立得

$$a_0=a_1=\cdots=a_{n-1}=0, \qquad b_0=(-1)^m.$$

于是由结式(1)立刻算出

$$\mathrm{Res}_y(f(y), g(y)) = (-1)^{mn}.$$

显然

$$\prod_{i,j}(0-1)=(-1)^{mn},$$

故$c=1$，即

$$\text{Res}_y(f(y),g(y)) = \prod_i \prod_j (x_i - z_j). \quad \blacksquare$$

系 1 如果

$$f(y) = a_n \prod_i (y - x_i), \quad g(y) = b_m \prod_j (y - z_j),$$

则有

$$\text{Res}_y(f(y),g(y)) = a_n^m b_m^n \prod_i \prod_j (x_i - z_j) = a_n^m \prod_i g(x_i)$$

$$= (-1)^{mn} b_m^n \prod_j f(z_j). \quad \blacksquare$$

系 2 设$\alpha_i, \beta_j \in K(i = 1, \cdots, n, j = 1, \cdots, m)$，如果

$$f(y) = a_n \prod_i (y - \alpha_i), \quad g(y) = b_m \prod_j (y - \beta_j),$$

则有

$$\text{Res}_y(f(y),g(y)) = a_n^m b_m^n \prod_i \prod_j (\alpha_i - \beta_j) = a_n^m \prod_i g(\alpha_i)$$

$$= (-1)^{mn} b_m^n \prod_j f(\beta_j).$$

证明 系 1 的等式是恒等式，以α_i替换变数x_i，以β_j替换变数z_j即可。 ▌

以下我们引入微分的概念。

定义3.14 设 $f(y) = \sum_i a_i y^i \in K[y]$，此处$K$是域。则$f(y)$的导数定义为

$$f'(y) = \sum_i i a_i y^{i-1}.$$

定理3.19 导数遵守常见的微分学的定律如下：

1） $(c)' = 0$，此处 $c \in K$；

2） $(af(y) + bg(y))' = af'(y) + bg'(y)$；

3） $(f(y)g(y))' = f'(y)g(y) + f(y)g'(y)$。

证明 读者自证。▍

定理3.20 设

$$f(y)=a_n\prod_{i=1}^{n}(y-\alpha_i),\qquad \alpha_i\in K.$$

我们定义$f(y)$的**判别式**$\mathrm{dis}(f(y))$为$\mathrm{Res}_y(f(y),f'(y))$。则有

$$\mathrm{dis}(f(y))=a_n^{m+n}\prod_{i\neq j}(\alpha_i-\alpha_j).$$

于是$f(y)$有重根的充要条件是$f(y)$的判别式$\mathrm{dis}(f(y))=0$，也即$f(y)$与$f'(y)$有次数大于零的公因元。

证明 显然，仅须证明

$$\mathrm{Res}_y(f(y),f'(y))=a_n^{m+n}\prod_{i\neq j}(\alpha_i-\alpha_j).$$

根据上面的定理，知

$$(*)\qquad \mathrm{Res}_y(f(y),f'(y))=a_n^m\prod_i f'(\alpha_i),$$

而且有

$$f'(y)=\left(a_n\prod_{i=1}^{n}(y-\alpha_i)\right)'=a_n\left(\sum_i\prod_{j\neq i}(y-\alpha_j)\right).$$

于是

$$f'(\alpha_i)=a_n\left(\sum_i\prod_{j\neq i}(\alpha_i-\alpha_j)\right)=a_n\prod_{j\neq i}(\alpha_i-\alpha_j).$$

将此式代入$(*)$即得本定理。▍

例7 1）设$f(y)=y^2-by+c$，则有

$$\mathrm{dis}(f(y))=\det\begin{bmatrix}1&-b&c\\2&-b&0\\0&2&-b\end{bmatrix}$$

$$=b^2-2b^2+4c=-b^2+4c=-\Delta,$$

此处△是一般所谓的二次方程的判别式。如令

$$f(y)=(y-a_1)(y-a_2),$$

则有

$$b=a_1+a_2,\qquad c=a_1a_2,$$

$$\begin{aligned}\operatorname{dis}(f(y))&=(a_1-a_2)(a_2-a_1)\\&=-(a_1+a_2)^2+4a_1a_2=-b^2+4c.\end{aligned}$$

2）设 $f(y)=y^3-ay^2+by-c=(y-a_1)(y-a_2)(y-a_3)$。则有

$$a=a_1+a_2+a_2,\qquad b=a_1a_2+a_2a_3+a_1a_3,\qquad c=a_1a_2a_3.$$

$$\operatorname{dis}(f(y))=\det\begin{pmatrix}1&-a&b&-c&0\\0&1&-a&b&-c\\3&-2n&b&0&0\\0&3&-2a&b&0\\0&0&3&-2a&b\end{pmatrix}$$

$$=4a^3c-a^2b^2-18abc+4b^3+27c^2.$$

也即

$$\begin{aligned}&-(a_1-a_2)^2(a_2-a_3)^2(a_1-a_3)^2\\&\quad=4(a_1+a_2+a_3)^3a_1a_2a_3\\&\qquad-(a_1+a_2+a_3)^2(a_1a_2+a_2a_3+a_1a_3)^2\\&\qquad-18(a_1+a_2+a_3)(a_1a_2+a_2a_3+a_3a_1)a_1a_2a_3\\&\qquad+4(a_1a_2+a_2a_3+a_1a_3)^3+27(a_1a_2a_3)^2.\end{aligned}$$

例 8 本节的主旨似乎仅在一元多项式，然而其实际的应用，可以解决多元多项式的问题。我们试取一例。在 $\boldsymbol{R}[x,y]$中任取两多项式 $f(x,y)$与 $g(x,y)$。经过线性变换，选取坐标，不妨假设如下：

$$\deg_{x\,y}f(x,y)=\deg_y f(x,y)=n,$$

$$\deg_{x\,y}g(x,y)=\deg_y g(x,y)=m,$$

即

$$f(x,y)=a_n y^n+\sum_{i=1}^{n} f_i(x) y^{n-i}, \qquad \deg_x f_i(x)\leqslant i,$$

$$g(x,y)=b_m y^m+\sum_{j=1}^{m} g_j(x) y^{m-j}, \qquad \deg_x g_j(x)\leqslant j.$$

令 $L=R[x]$的比域 $=R(x)$，即一元有理函数域。在 $L[y]$中考虑 $f(x,y),g(x,y)$的结式

$$\operatorname{Res}_y(f(x,y),g(x,y))$$

$$=\det\begin{pmatrix} a_n & f_1(x) & \cdots & f_n(x) & 0 & 0 & \cdots & 0\\ 0 & a_n & \cdots & f_{n-1}(x) & f_n(x) & 0 & \cdots & 0\\ & & \cdots & \cdots & \cdots & \cdots & & \\ & & & \cdots & \cdots & \cdots & \cdots & \\ 0 & 0 & \cdots & \cdots & a_n & f_1(x) & \cdots & f_n(x)\\ b_m & g_1(x) & \cdots & \cdots & g_{m-1}(x) & g_m(x) & \cdots & 0\\ & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0 & \cdots & b_m & g_1(x) & \cdots & \cdots & \cdots & g_m(x)\end{pmatrix}.$$

不难仿照定理3.18的第一步骤的证明，证出

$$\deg_x(\operatorname{Res}_y(f(x,y),g(x,y)))\leqslant nm.$$

上面这个不等式有很好的几何意义，我们阐明如下：如果 $x=\alpha$，$y=\beta$ 是在由下列两个方程式

$$f(x,y)=0, \quad g(x,y)=0$$

所定义的曲线的交点上，则

$$f(\alpha,y)=0 \quad 与 \quad g(\alpha,y)=0$$

有公解。也即

$$\operatorname{Res}_y(f(\alpha,y),g(\alpha,y))=0.$$

于是 $\operatorname{Res}_y(f(x,y),g(x,y))$的根是此两条曲线的交点在 x 轴上的“投影”。同理可以证出，由方程式

$$\operatorname{Res}_z(f(x,y,z),g(x,y,z))=0$$

所定义的曲线是 $f(x,y,z)=0$ 与 $g(x,y,z)=0$ 所定义的两个曲面的交线在 (x,y) 平面上的投影。我们再回过头来研究二元多项式的情形。上面的那个不等式

$$\deg_x(\operatorname{Res}_y(f(x,y),g(x,y)))\leqslant nm$$

说明：如果 $\operatorname{Res}_y(f(x,y),g(x,y))$ 不是零多项式时，此两曲线在 x 轴上最多只有 nm 个投影点。于是我们有：

贝朱定理 如果两多项式 $f(x,y),g(x,y)$ 无次数大于零的公因子，则它们定义的两曲线最多有 nm 个交点，此处

$$n=\deg_{x,y}f(x,y),\qquad m=\deg_{x,y}g(x,y).$$

证明 设有多于 mn 个交点。用直线连接其中 $nm+1$ 个点。选取 x,y 轴，使 y 轴适合前面所提到的条件，即不与这些连接线相平行。如此，则此 $nm+1$ 个点在 x 轴上的投影皆不相同。根据上面的讨论，这是不可能的。所以此两曲线最多只有 nm 个交点。▎

朱世杰在《四元玉鉴》(1303年)中，开始研究多元多项式，从二元到四元多项式。其中有所谓“上升下降，左右进退，互通变化，乘除往来，用假像真，以虚问实”，又有“寄之、剔之、余筹易位，横冲直撞，精而不杂，自然而然，消而和会”。其目的是“以成开方之式(一元多项式)也”。这是各种移项变换及消元法，最后归结成一元多项式。朱世杰发明的方法与本书的定理3.8及定理3.17很有关系。

西方开始系统地研究多元多项式的数学家是十八世纪的法国人贝朱。

习 题

1. 设 K 是特征为 0 的域。任取 $f(x)\in K[x]$，证明

$$f'(x)=0\iff f(x)\in K.$$

如果 K 的特征 $=p>0$，证明 $f'(x)=0\iff$ 存在多项式 $g(x)\in K[x]$，使 $f(x)=g(x^p)$。

2. 在形式幂级数环 $K[[x]]$ 中，我们也可以定义导数如下：令 $f(x)=\sum_i a_i x^i$，定义

$$f'(x)=\sum_{i=1}^{+\infty} i a_i x^{i-1}.$$

证明$K[[x]]$内的上述导数也有定理3.19的三条性质。

3. 利用定义 $(g^{-1}(x))'=-g^{-2}(x)g'(x)$，把导数的定义推广到$K(x)$及$K((x))$。

4. 证明$f(x)=1+x+\frac{x^2}{2!}+\cdots+\frac{x^n}{n!}\in \boldsymbol{R}[x]$没有重根。

5. 设域K包含无穷多个元素，$f(x_1,\cdots,x_n)\in K[x_1,\cdots,x_n]$。证明如对$K$内任意 $a_1,\cdots,a_n$ 都有$f(a_1,\cdots,a_n)=0$，则 $f=0$。换句话说，设域 K 包含无穷多个元素，$f(x_1,\cdots,x_n)\in K[x_1,\cdots,x_n]$，且 $f\neq 0$。则必存在$a_1,\cdots,a_n\in K$，使$f(a_1,\cdots,a_n)\neq 0$。

6. 以$\alpha_1,\cdots,\alpha_n$表示变元$x_1,\cdots,x_n$的初等对称多项式，而

$$s_k=x_1^k+x_2^k+\cdots+x_n^k \quad (k=1,2,\cdots).$$

证明牛顿公式

$$s_m-\alpha_1 s_{m-1}+\alpha_2 s_{m-2}-\cdots+(-1)^{m-1}\alpha_{m-1}s_1 +(-1)^m m\alpha_m=0 \quad (m\leqslant n),$$

$$s_m-\alpha_1 s_{m-1}+\alpha_2 s_{m-2}-\cdots+(-1)^n s_{m-n}\alpha_n=0 \quad (m>n).$$

7. 续上题。设 s_m表示成初等对称多项式$\alpha_1,\cdots,\alpha_n$的多项式

$$s_m=\sum_{l_1+2l_2+\cdots+nl_n=m} a_{l_1\cdots l_n}\alpha_1^{l_1}\alpha_2^{l_2}\cdots\alpha_n^{l_n}.$$

证明其系数满足

$$a_{l_1\cdots l_n}=(-1)^l m\frac{(l_1+l_2+\cdots+l_n-1)!}{l_1!l_2!\cdots l_n!},$$

其中 $l=l_2+l_4+\cdots+l_{2[n/2]}$。

8. 求多项式 $f(x)=x^n-a$ 和 $g(x)=x^n+ax+b(n\geqslant 2)$ 的判别式。

9. 求 $f(x)=x^{12}+2x^{11}+x^{10}+x^3+x^2-x-1$ 的判别式。

10. 设 $f(x),g(x)$ 是域 K 上的两个一元多项式，证明

$$\mathrm{Res}_x(f,g)=(-1)^{mn}\mathrm{Res}_x(g,f),$$

其中 $m=\deg f$，$n=\deg g$。又设 $g_1,g_2\in K[x]$，证明

$$\mathrm{Res}_x(f,g_1g_2)=\mathrm{Res}_x(f,g_1)\cdot\mathrm{Res}_x(f,g_2).$$

11. 考虑 $f(x)=x^3+4x^2-x-4$ 的判别式 $\mathrm{dis}(f)$，求所有的素数 p，使 $f(x)\pmod p$ 有重根。

12. 求 $x^2+xy+z^2=0$ 及 $x^2-y-z^3=0$ 的交线在 X-Y 平面上的投影。

13. 求下列二元联立方程组的整数解：

$$\begin{cases}5y^2-6xy+5x^2-16=0,\\ y^2-xy+2x^2-y-x-4=0.\end{cases}$$

14. 用初等对称多项式表示 $x_1,x_2,\cdots,x_n$ 的对称函数

$$\sum_{i<j<k}(x_i-x_j)^2(x_i-x_k)^2(x_j-x_k)^2.$$

§5 理　　想

在第一章的§2、§5及本章的§3中，我们已屡次用到一集合 $(f_1,f_2,\cdots,f_m)$。我们用下面的定义给它定名。

定义3.15 设 R 为一环。A 为 R 的一非空子集。A **生成的理想**定义为

$$\left\{\sum_{\text{有限}}r_ia_ir_i':\ r_i,r_i'\in R,\ a_i\in A\right\},$$

用符号 (A) 表示之。如果 $A=\{a_1,a_2,\cdots,a_m\}$ 为一有限集，则 A 生成的理想 (A) 也用 $(a_1,a_2,\cdots,a_m)$ 表示之。当 $(I)=I$ 时，则称

I 为理想。

一个环R的理想I与一个群G的正规子群N的位置相当，即两者都是映射的核。我们阐述如下。

定义 3.16 设$\rho: R \to R'$为环R到环R'的映射。如果ρ保持运算关系，即对所有的$r_1, r_2 \in R$，都有

$$\rho(r_1 + r_2) = \rho(r_1) + \rho(r_2), \qquad \rho(r_1 \cdot r_2) = \rho(r_1) \cdot \rho(r_2),$$

则称ρ为R到R'的**一环映射**。

定义3.17 设ρ: $R \to R'$为一环映射。如ρ为单射，则称ρ为**环单射**。如ρ为满射，则称ρ为**环满射**，或称R'为R**的映象**。如ρ为单满映射，则称ρ为一同构，此时称R与R'**是同构的**，用$R \simeq R'$表示之。如果ρ为同构，且有$R = R'$，则称ρ为**自同构**。

定义 3.18 设ρ为环R到环R'的一环映射。ρ**的象** $\text{im}(\rho)$的定义如下：

$$\text{im}(\rho) = \{r': \text{存在 } r \in R, \text{ 使得} \rho(r) = r'\}。$$

ρ的**核**$\ker(\rho)$的定义如下：

$$\ker(\rho) = \{r: \rho(r) = 0', \ 0'\text{是}R'\text{的零元}\}。$$

换言之，$\ker(\rho)$是$0'$的象源，也可以用$\rho^{-1}(0')$表示之。

定理 3.21 1) 设ρ: $R \to R'$为一环映射。则$\ker(\rho)$是R的一理想；

2) 令I为R的理想，则下述关系"$\sim$"

$$r_1 \sim r_2 \iff r_1 - r_2 \in I$$

是一等价关系。令其商集为R/I，则R/I在如下的自然的加法（"+"）与乘法（"·"）的运算下，自然成为一环，即所谓R对I**的商环**：

$$[r_1] + [r_2] = [r_1 + r_2], \qquad [r_1] \cdot [r_2] = [r_1 \cdot r_2],$$

此处$[r]$表示r所在的等价子集；

3) 令σ: $R \to R/I$的定义为$\sigma(r) = [r]$。则σ是一环满射，且$\ker(\sigma) = I$。

证明 1) 任取

$$a \in (\ker(\rho)) = \left\{ \sum_i r_i a_i r_i' : r_i, r_i' \in R,\ a_i \in \ker(\rho) \right\},$$

则有

$$\rho(a) = \rho\left(\sum_i r_i a_i r_i'\right) = \sum_i \rho(r_i)\rho(a_i)\rho(r_i')$$

$$= \sum_i \rho(r_i) \cdot 0 \cdot \rho(r_i') = 0,$$

即 $a \in \ker(\rho)$。于是有 $(\ker(\rho)) \subset \ker(\rho)$。反之，显然有 $(\ker(\rho)) \supset \ker(\rho)$，故 $(\ker(\rho)) = \ker(\rho)$，即 $\ker(\rho)$ 是 R 的一理想。

2) 我们先验证 $\sim$ 是个等价关系。

(a) $r_1 \sim r_2 \Longrightarrow r_1 - r_2 \in I \Longrightarrow (-1)(r_1 - r_2) \in (I) = I \Longrightarrow r_2 - r_1 \in I \Longrightarrow r_2 \sim r_1$； (对称性)

(b) 由于 I 是非空的，可取 $a \in I$。则 $0 = 0 \cdot a \in (I) = I$。于是 $r_1 \sim r_1$； (反身性)

(c) $r_1 \sim r_2$， $r_2 \sim r_3 \Longrightarrow r_1 - r_2 \in I$， $r_2 - r_3 \in I \Longrightarrow r_1 - r_3 = (r_1 - r_2) + (r_2 - r_3) \in (I) = I \Longrightarrow r_1 \sim r_3$。 (传递性)

于是 $\sim$ 是一等价关系。对于加法及乘法的运算，我们仅仅证明它们是有意义的，读者自证其余环的规则。现在我们证明

$$[r_1] = [r_1'],\ [r_2] = [r_2'] \Longrightarrow [r_1 + r_2] = [r_1' + r_2'] \text{ 及 } [r_1 \cdot r_2] = [r_1' \cdot r_2'].$$

这就是所谓“定义是有意义的”。证法如下：

$$\begin{aligned} &[r_1] = [r_1'],\ [r_2] = [r_2'] \\ &\quad \Longrightarrow r_1 - r_1' = a_1 \in I,\ r_2 - r_2' = a_2 \in I \\ &\quad \Longrightarrow (r_1 + r_2) - (r_1' + r_2') = a_1 + a_2 \in (I) = I, \\ &\qquad r_1 \cdot r_2 - r_1' \cdot r_2' = a_1 r_2' + a_2 r_1' + a_1 a_2 \in (I) = I \\ &\quad \Longrightarrow [r_1 + r_2] = [r_1' + r_2'],\quad [r_1 \cdot r_2] = [r_1' \cdot r_2']. \end{aligned}$$

3) 显然。读者自证。 ▎

与群论一样，我们有下列的“同构定理”。

定理 3.22 令 ρ: $R \to R'$ 为一环满射。设 I' 为 R' 的一个理想，令 $I = \{r: \rho(r) \in I'\}$。则有

1) I 是 R 的理想，$I \supset \ker(\rho)$；

2) 定义 $\bar{\rho}$: $R/I \to R'/I'$ 如下：任取 $[r] \in R/I$，令

$$\bar{\rho}\,[r] = [\rho(r)] \in R'/I'.$$

则 $\bar{\rho}$ 是一个同构。

证明 1) 任取

$$a = \sum_i r_i a_i r'_i \in (I) = \left\{ \sum_i r_i a_i r'_i : a_i \in I,\ r_i, r'_i \in R \right\}$$

则有

$$\rho(a) = \sum_i \rho(r_i)\rho(a_i)\rho(r'_i) \in (I') = I',$$

即 $a \in I$。于是不难看出，$I = (I)$，即 I 是一个理想。又，任取 $a \in \ker(\rho)$，则有 $\rho(a) = 0' \in I'$，故 $a \in I$，即有 $I \supset \ker(\rho)$。

2) 读者参考定理 3.21 的 2)的证明，试自证之。▌

系 如 ρ: $R \to R'$ 是一环满射，则有

$$R/\ker(\rho) \approx R'.$$

证明 取 $I' = (0)$，不难看出，$R'/(0) \approx R'$。▌

例 9 设 K 为域。不妨设想 $K = \mathbf{Q}, \mathbf{R}$ 或 $\mathbf{C}$。考虑一元多项式环 $K[x]$。令 $I = (x - a)$，此处 $a \in K$。经过变数变换 $u = x - a$，$K[x] = K[u]$。为简便起见，不妨即令 $a = 0$。此时有

$$\sigma: K[x] \to K[x]/(x).$$

映射 σ 是什么？令 $f(x) = b_0 + b_1 x + \cdots + b_n x^n$，则

$$f(x) - f(0) = f(x) - b_0 = (b_1 + \cdots + b_n x^{n-1})x \in (x),$$

即 $f(x) \sim f(0)$。不难看出

$$\sigma(f(x)) = \sigma(f(0)) = [f(0)].$$

而且有如下定义的映射 λ 为满单映射：

$$\lambda:\ K[x]/(x)\approx K,$$
$$\lambda(f[0])=f(0)。$$

借助同构 λ 把 $K[x]/(x)$ 与 K 等同看待，则映射 σ 与 $f(x)$ 在原点取值实无甚差别。多项式 $f(x)$ 在某一指定的点 $x=a$ 取值，可以看成映射

$$K[x]\to K[x]/(x-a)\approx K。$$

同理，在多元多项式环 $K[x_1,\cdots,x_n]$ 中，多项式 $f(x_1,\cdots,x_n)$ 在 $x_1=a_1,\cdots,x_n=a_n$ 点取值，也可以考虑成映射

$$K[x_1,\cdots,x_n]\to K[x_1,\cdots,x_n]/(x_1-a_1,\cdots,x_n-a_n)\approx K。$$

例10 令 $A\subset K[x_1,\cdots,x_n]$，此处 K 是域。读者不妨即假想 $K=\mathbf{Q},\mathbf{R}$ 或 $\mathbf{C}$。我们考虑下面一组方程式的公解：

(1) $$f_i(x_1,\cdots,x_n)=0,\qquad \forall f_i\in A。$$

如果 $x_1=a_1,\cdots,x_n=a_n$ 适合上面的所有方程式，则也必适合下面的所有方程式

$$g(x_1,\cdots,x_n)=\sum_{\text{有限}}h_i(x_1,\cdots,x_n)f_i(x_1,\cdots,x_n)=0。$$

其中 $h_i\in K[x_1,\cdots,x_n]$，$f_i\in A$。即适合

(2) $$g(x_1,\cdots,x_n)=0,\qquad \forall g\in(A)。$$

反之，因为 $A\subset(A)$，显然(2)的公解也是(1)的公解。于是(1)与(2)的公解是完全相同的。

我们举一些应用。谁都知道，不同的两个圆最多相交于两点。我们给一简单的代数证明如下。设此两圆的方程式为

$$f(x,y)=x^2+y^2+a_1x+a_2y+a_3=0,$$
$$g(x,y)=x^2+y^2+b_1x+b_2y+b_3=0。$$

两者相减，得

$$\begin{aligned}h(x,y)&=f(x,y)-g(x,y)\\&=(a_1-b_1)x+(a_2-b_2)y+(a_3-b_3)=0。\end{aligned}$$

不难看出，$h(x,y)$ 并非零多项式，而且有

$$(f(x,y),g(x,y))=(f(x,y),h(x,y))。$$

根据贝朱定理，$f(x,y)=0$与$h(x,y)=0$最多只有两个交点．于是$f(x,y)=0$与$g(x,y)=0$最多只有两个交点．

进一步说，在上面这个例子中，如果$f(x,y)=0$与$h(x,y)=0$有两个交点，则$h(x,y)=0$即是通过这两点的直线的方程式．又如果此圆与此直线仅有一个交点，则原来给定的两圆必定相切，而$h(x,y)=0$即是两圆公共切线的方程式．

例11 在例10中，我们考虑的是求一组方程式的公解，我们也可以反其道而行之：先给定

$$\boldsymbol{R}^n=\boldsymbol{R}\times\boldsymbol{R}\times\cdots\times\boldsymbol{R}=\{(r_1,r_2,\cdots,r_n):\ r_i\in\boldsymbol{R}\}$$

的一个子集T，然后考虑$\boldsymbol{R}[x_1,x_2,\cdots x_n]$中在$T$的所有点均取零值的多项式的集合$I$，即

$$I=\{f(x_1,\cdots,x_n):\ f(a_1,\cdots.a_n)=0,\forall(a_1,\cdots,a_n)\in T\}.$$

不难看出

$$(I)=I,$$

即I是一个理想．如果我们反过来求I的公解，则立得

$$I\text{的公解}\supset T.$$

一般言之，上面这个包含式的左右两侧并不相等．如果两者相等，则称T是一个**代数多样体**(或**代数子集**、**代数簇**)．

我们取一个非代数子集的例子．令$n=1$，

$$T=\{r_1:\ r_1\geqslant 0,\ r_1\in\boldsymbol{R}\}.$$

因为T中有无限多个点，而任一非零多项式$f(x_1)$只有有限多个根，于是有

$$I=\{f(x_1):\ f(r_1)=0,\ \forall r_1\geqslant 0,\ r_1\in\boldsymbol{R}\}=(0).$$

而方程式

$$0=0$$

的公解是$x_1=r$，$\forall r\in\boldsymbol{R}$，即

$$I\text{的公解}=\boldsymbol{R}\supsetneqq T.$$

于是T不是一代数子集，或代数多样体．▌

从上面这些例子，读者可以看出，理想是很重要的代数概念。于是，我们把理想加以分类，以便研究。我们有：

定义3.19 1）由一个元素生成的理想(a)称为主理想；

2）设R为一交换环，I为一理想。如果$I\neq R$，并且任一包含I的理想必为I或R，则称I为一极大理想；

3）设R为一交换环，I为一理想。如果$I\neq R$，且对任意的元素a,b，当$a\cdot b\in I$时，必有$a\in I$或$b\in I$，则称I为素理想。

例12 在域K中，唯一的极大理想是(0)。事实上，在任意域K中，只有两个理想：(0)及K。于是，(0)也是域K的唯一的素理想。

反之，设交换环R中仅有两个理想(0)及K，则我们可以证明R必为域：任取$0\neq a\in R$，因为$(a)\ni a$，所以$(a)\neq(0)$，于是$(a)=R$，故$1\in(a)$，即存在$b\in R$，使$ab=1$。自然，b是a的乘法逆元素。如此得出R中每一非零元素a皆有乘法逆元素。不难从此导出R是域。

在$\mathbf{C}[x,y]$中，$(x-a,y-b)$是极大理想，此处$a,b\in\mathbf{C}$。而$(x-a)$是素理想，这不难自"$x-a$是素元"的事实直接导出。

定理3.23 设R为一交换环，则R中最少有一极大理想。设$a\in R$，具有下述性质：

$$a^i\neq 0,\quad i=1,2,\cdots,n,\cdots,$$

则有一素理想I，使得$a\overline{\in} I$。

证明 我们先证明后半部分。在以下的证法中，令$a=1$，则立得前半部分。

我们用Zorn引理。令

$$\mathscr{F}=\{I:\ I\text{是理想},\ a^i\overline{\in} I,\ i=1,2,\cdots,n,\cdots\}.$$

显然有$(0)\in\mathscr{F}$，所以$\mathscr{F}$非空集。在$\mathscr{F}$中定义半序"$\leqslant$"：

$$I_1\leqslant I_2\iff I_1\subset I_2.$$

我们要证明$\mathscr{F}$中的任意链$\{I_j\}$必有上限。取

$$I=\bigcup_j I_j,$$

读者试证I是一理想。我们仅证$a^i\overline{\in}I$，$i=1,2,\cdots,n,\cdots$。假若$a^n\in I$，我们将导出一矛盾。因为$I=\bigcup_j I_j$，所以必有一适当的m，使$a^n\in I_m$，这与I_m的定义相违。如此，我们得出$I\in\mathscr{F}$。

根据Zorn引理，在$\mathscr{F}$中有一极大元素I（并不一定是一个极大理想）。设$b\cdot c\in I$。假若b和c都不属于I，由于I的极大性，则两个理想

$$(b)+I=\{db+i:\ d\in R,\ i\in I\}$$

及
$$(c)+I=\{dc+i:\ d\in R,\ i\in I\}$$

都不属于$\mathscr{F}$。即有m,l及r,s存在，使

$$a^m=d_1b+r,\qquad m>0,\ r\in I,$$

$$a^l=d_2c+s,\qquad l>0,\ s\in I.$$

两式相乘，得

$$a^{m+l}=(d_1d_2)b\cdot c+d_1bs+d_2cr+rs\in I.$$

此是一矛盾。所以，如果$b\cdot c\in I$，必有$b\in I$或$c\in I$，即I是素理想。

在以上证法中，令$a=1$，如法取$\mathscr{F}$的极大元素I。如果一理想$J\supsetneqq I$，则必有$J\ni 1^n=1$，于是J必为R。所以理想I是一个极大理想。∎

定理3.24 1）设R是一交换环，I是一理想。则I是极大理想的充要条件是R/I为域；

2）设R是一交换环，I是一理想。则I是素理想的充要条件是R/I为整环。

证明 1）参考例12。我们令ρ: $R\to R/I$为（典型的）环满射。如果J为R/I的理想，则$\rho^{-1}(J)$（即J的象源）是R的理

想。反之，设理想 $J\supset I$，则 $\rho(J)$（即 J 的象）是 R/I 的理想。于是，有

$$R/I\text{ 是域}\Longleftrightarrow R/I\text{ 仅有}(\bar{0})\text{及 }R/I\text{ 两个理想}$$
$$\Longleftrightarrow\text{理想 }J\supseteq I\text{ 时，必有 }J=I\text{ 或 }J=R$$
$$\Longleftrightarrow I\text{ 为极大理想。}$$

2) $\Longrightarrow$。任取 $\bar{a},\bar{b}\in R/I$，我们令 $\bar{a}=\rho(a)$， $\bar{b}=\rho(b)$。则有

$$\bar{a}\cdot\bar{b}=0\Longleftrightarrow a\cdot b\in I\Longleftrightarrow a\in I\text{ 或 }b\in I$$
$$\Longleftrightarrow\bar{a}=\bar{0}\text{ 或 }\bar{b}=\bar{0}.$$

$\Longleftarrow$。设 $a\cdot b\in I$。则 $\bar{a}\cdot\bar{b}=\bar{0}$。因为 R/I 是整环，所以必有 $\bar{a}=\bar{0}$或 $\bar{b}=\bar{0}$。即 $a\in I$ 或 $b\in I$。▎

系 任一极大理想 I 必是素理想。

从例10及定理1.4，定理1.15及定理3.9等处，我们不难体会，一个理想 I 可以有许多不同的生成元集。这些生成元集有良莠之别，而其基数也有多寡之分。有一类特别简单的环是“主理想环”，定义如下。

定义3.20 设 R 为一交换环。如果 R 中的理想皆为主理想，即皆由一个元素生成的，则称 R 为**主理想环**。如果 R 同时又为整环，则称 R 为**主理想整环**。

例13 零环是主理想环，但不是主理想整环。设 K 是任意域，则 K 仅有两个理想：(0)以及 $K=(1)$。故 K 是一个主理想整环。

如上，设 K 是域。考虑 $K[x]$，$\boldsymbol{Z}$ 以及 $\boldsymbol{Z}[i]$。定理1.4，定理1.15及定理3.9显示了其中有限生成的理想都是主理想。其实，我们可以用同一方法证明，$K[x]$，$\boldsymbol{Z}$ 及 $\boldsymbol{Z}[i]$的任意理想都是主理想。我们证明 $K[x]$的情形，读者自证 $\boldsymbol{Z}$ 及 $\boldsymbol{Z}[i]$的情形。

设$(0)\neq I$ 是 $K[x]$的一个理想。令 $d(x)$为 $I\backslash\{0\}$中次数最低的多项式。任取 $f(x)\in I\backslash\{0\}$，则根据定理3.9，存在 $g(x)\in$

$K[x]$，使得 $(d(x),f(x))=(g(x))$。显然，我们有

1) $g(x)\in(d(x),f(x))\subset I$；

2) $g(x)\mid d(x)\Longrightarrow \deg g(x)\leqslant \deg d(x)$；

然而 $d(x)$ 的次数已是最低的了，所以必有

3) $\deg g(x)=\deg d(x)\Longrightarrow d(x)=ag(x)$，$a\in K\setminus\{0\}$。

也即 $d(x)$ 与 $g(x)$ 为相伴元素。如此立得 $d(x)\mid f(x)$，即 $f(x)\in(d(x))$。故有 $(d(x))=I$。这样，我们证明了 $K[x]$ 是主理想整环。

作为非主理想环的例子，我们考虑 $K[x,y]$。令 $I=(x,y)$，则 I 并非一主理想。所以 $K[x,y]$ 不是主理想环。 ▎

以下我们讨论与多元多项式环 $K[x_1,x_2,\cdots,x_n]$ 极有关系的某一类环。

定义3.21 设 R 为一交换环。如果 R 的任一理想 I 皆可由有限子集生成，则称 R 为**诺德环**。

以下的定理给出诺德环的不同的判别条件。

定理3.25 设 R 为一交换环。则下列三条是等同的：

1) R 的任一理想皆可由有限子集生成；

2) R 的理想的上升的链必然终止，即，如有下列的链：

$$I_1\subset I_2\subset\cdots\subset I_n\subset I_{n+1}\subset\cdots,$$

其中 I_n 皆是理想，则必存在一 m，使

$$I_m=I_{m+1}=\cdots;$$

3) **极大原则**：如果 $\mathscr{F}$ 是 R 的理想的一个非空集合，则 $\mathscr{F}$ 中必有一极大的理想，即，存在一个理想 $I\in\mathscr{F}$，使

$$I\subset J\in\mathscr{F}\Longrightarrow I=J.$$

证明 我们采取循环证法：1)$\Longrightarrow$2)$\Longrightarrow$3)$\Longrightarrow$1)。

1)$\Longrightarrow$2)．如有下列上升的链

$$I_1\subset I_2\subset\cdots\subset I_n\subset I_{n+1}\subset\cdots,$$

令
$$I=\bigcup_{i=1}^{\infty}I_i.$$

我们先证 I 是理想。令

$$g=\sum_{\text{有限}} h_i f_i,$$

其中 $f_i \in I$, $h_i \in R$。因为 I 是 $I_1, I_2, \cdots, I_n, \cdots$ 的并集，所以 $f_i \in I_{n_i}$，此处 n_i 是适当的指标。取 $m > n_i, \forall i$，则有 $f_i \in I_m$, $\forall i$。因为 I_m 是理想，故有

$$g=\sum_i h_i f_i \in (I_m) = I_m \subset I,$$

即 $(I) \subset I$。又恒有 $(I) \supset I$，于是得出 $(I)=I$，也即 I 是一理想。

我们假设 R 适合条件 1），则 I 有一个有限的生成子集。令 $I=(g_1, g_2, \cdots, g_l)$。应用与上面相同的方法，可证存在一 m，使 $g_i \in I_m$, $\forall i=1,2,\cdots,l$。于是 $I=I_m=I_{m+1}=\cdots$。

2）$\Longrightarrow$ 3）。我们假设 R 适合条件 2)，要证明 R 必适合条件 3）。如 $\mathscr{F}$ 是 R 的理想的一个非空的集合。在 $\mathscr{F}$ 中任取一理想 I_1。如果 I_1 并非极大，则在 $\mathscr{F}$ 中存在一 I_2，使

$$I_1 \subsetneqq I_2.$$

如 I_2 在 $\mathscr{F}$ 中并非极大，则在 $\mathscr{F}$ 中存在一 I_3，使

$$I_1 \subsetneqq I_2 \subsetneqq I_3.$$

如此反复选取 $I_4, I_5, \cdots, I_n, \cdots$。根据 2），理想的上升的链必然终止，故知经过有限次数后，必然取得 $\mathscr{F}$ 中的一极大理想。

3）$\Longrightarrow$ 1）。我们假设"极大原则"，然后求证 1)。设 I 是 R 的一理想。在 I 中任取一元素 f_1，则有 $(f_1) \subset I$。如两者不等，则任取 $f_2 \in I \backslash (f_1)$。显然有

$$(f_1) \subsetneqq (f_1, f_2) \subset I.$$

如果 $I \neq (f_1, f_2)$，则任取 $f_3 \in I \backslash (f_1, f_2)$。经过 n 次选取 $f_1, f_2, \cdots, f_n$ 以后，我们有

$$(f_1) \subsetneqq (f_1, f_2) \subsetneqq \cdots \subsetneqq (f_1, f_2, \cdots, f_n) \subset I.$$

如果始终恒有

$$I \subsetneqq (f_1, f_2, \cdots, f_n),$$

则令

$$\mathscr{F} = \{(f_1),(f_1,f_2),\cdots,(f_1,f_2,\cdots,f_n),\cdots\}.$$

在此非空集合$\mathscr{F}$中，显然沒有极大的理想．此与“极大原则”相矛盾。于是得出，经过有限步骤后，存在一m，使

$$I=(f_1,f_2,\cdots,f_m),$$

即I是由有限子集生成的。▌

从下面这个定理，立得n元多项式环$K[x_1,x_2,\cdots,x_n]$是诺德环。

定理3.26（希尔伯特基定理） 设R是诺德环，则一元多项式环$R[x]$也是诺德环。

证明 任取$R[x]$的一理想I，我们要证明I有一个有限生成子集．令

$$I_n=\{a_n:\ 存在\ a_0+a_1x+\cdots+a_nx^n\in I\}.$$

我们先证I_n是R的理想。

任取$b\in(I_n)$，令

$$b=\sum_{有限}c_ia_{ni},\qquad c_i\in R,\ a_{ni}\in I_n.$$

设与a_{ni}对应的多项式为

$$a_{0i}+a_{1i}x+\cdots+a_{ni}x^n\in I,$$

则立得$\sum_i c_i(a_{0i}+a_{1i}x+\cdots+a_{ni}x^n)\in I$．故$b=\sum_i c_ia_{ni}\in I_n$。

于是I_n是R的理想。

如$a_n\in I_n$，令与其对应的多项式为$a_0+a_1x+\cdots+a_nx^n\in I$，则

$$x(a_0+a_1x+\cdots+a_nx^n)=a_0x+a_1x^2+\cdots+a_nx^{n+1}\in I.$$

于是有$a_n\in I_{n+1}$。故$I_n\subset I_{n+1}$。如此，我们得出R的理想的一个上升的链：

$$I_0 \subset I_1 \subset I_2 \subset \cdots \subset I_n \subset I_{n+1} \subset \cdots.$$

因为R是诺德环，根据定理3.25，此链必然终止。即存在一m，使

$$I_m = I_{m+1} = \cdots.$$

以下，我们将选择I的一组有限生成子集。

因为R是诺德环，所以I_n都有有限生成子集。对$I_0, I_1, \cdots, I_m$，分别取它们的有限生成子集：

$$I_n = (a_{n1}, a_{n2}, \cdots, a_{nl_n}), \quad n = 0, 1, 2, \cdots, m.$$

令$f_{n1}, f_{n2}, \cdots, f_{nl_n}$为与其对应的多项式，即

$$f_{ni} = a_{(0)i} + a_{(1)i}x + \cdots + a_{ni}x^n \in I, \quad i = 1, 2, \cdots, l_n.$$

我们将证明$I = (f_{01}, \cdots, f_{0l_0}, f_{11}, \cdots, f_{1l_1}, \cdots, f_{m1}, \cdots, f_{ml_m})$.

任取$f(x) \in I$。令$f(x)$的展开式如下：

$$f(x) = a_0 + a_1x + \cdots + a_qx^q, \quad a_q \neq 0.$$

我们对$f(x)$的次数进行数学归纳法。如果$q = 0$，则

$$f(x) = a_0 \in I_0 = (f_{01}, \cdots, f_{0l_0}) \subset (f_{01}, \cdots, f_{ml_m}).$$

于是，我们假设对任何次数小于q的多项式$g(x)$，

$$g(x) \in I \Rightarrow g(x) \in (f_{01}, \cdots, f_{ml_m}).$$

如$q \leqslant m$，因为$a_q \in I_q = (a_{q1}, \cdots, a_{ql_q})$，所以存在$c_i (i = 1, 2, \cdots, l_q)$，使

$$a_q = \sum_i c_i a_{qi}.$$

于是，令

$$f(x) - \sum_i c_i f_{qi}(x) = g(x),$$

则有$g(x) \in I$及$\deg g(x) < q$。根据数学归纳法，就有

$$g(x) \in (f_{01}, \cdots, f_{ml_m}),$$

于是立得

$$f(x)=g(x)+\sum_i c_i f_{qi}(x)\in(f_{01},\cdots,f_{ml_m}).$$

如 $q>m$，因为 $a_q\in I_q=(a_{m1},\cdots,a_{ml_m})$，所以存在 $c_i(i=1,2\cdots,l_m)$，使

$$a_q=\sum_i c_i a_{mi}.$$

于是，令

$$f(x)-\left(\sum_i c_i f_{mi}(x)\right)x^{q-m}=g(x),$$

则有 $g(x)\in I$ 及 $\deg g(x)<q$。根据数学归纳法，有

$$g(x)\in(f_{01},\cdots,f_{ml_m}).$$

于是立得

$$f(x)=g(x)+\left(\sum_i c_i f_{mi}(x)\right)x^{q-m}\in(f_{01},\cdots,f_{ml_m}).\ \blacksquare$$

系 设K是域。则$K[x_1,x_2,\cdots,x_n]$是诺德环。

证明 因为K是主理想环，所以K是诺德环。用数学归纳法，令 $R=K[x_1,x_2,\cdots,x_{n-1}]$，则从本定理立得本系。$\blacksquare$

定理3.27 设R'是一个诺德环R的映象，则R'是诺德环。

证明 令 ρ: $R\to R'$是给定的映射。令

$$I_0=\ker(\rho).$$

我们将用定理3.25的第二个条件，即"上升的链必然终止"的条件，来证明R'是一个诺德环。

任取R'的理想的一个上升的链如下：

$$I'_1\subset I'_2\subset\cdots\subset I'_n\subset I'_{n+1}\subset\cdots.$$

令 $I_n=\rho^{-1}(I'_n)$，即 I'_n的象源。则有

$$I_0\subset I_1\subset I_2\subset\cdots\subset I_n\subset I_{n+1}\subset\cdots.$$

因为R是诺德环，所以存在m，使 $I_m=I_{m+1}=\cdots$。所以有

$$\rho(I_m)=\rho(I_{m+1})=\cdots,$$

即

$$I'_m=I'_{m+1}=\cdots.$$

这就证明了 R' 是一个诺德环。▌

例14 定理3.26及定理3.27证明了许多环都是诺德环。例如，我们在平面上取定一条代数曲线，为简便起见，即令此代数曲线为椭圆，而且其方程式为

$$x^2+a^2y^2-1=0,\quad a\in \boldsymbol{R},\quad a\neq 0.$$

令

$$I=(x^2+a^2y^2-1).$$

任取两多项式 $f(x,y),g(x,y)\in \boldsymbol{R}[x,y]$。如果有

$$h(x,y)=f(x,y)-g(x,y)\in I,$$

则显然，$f(x,y)$ 与 $g(x,y)$ 在椭圆上各点的值皆相等。反之，设此两多项式在椭圆上各点的值皆相等，我们要证明

$$h(x,y)=f(x,y)-g(x,y)\in I.$$

多项式 $x^2+a^2y^2-1$ 显然不能分解成一次式的乘积。如果 $h(x,y)\notin I$，则 $x^2+a^2y^2-1$ 与 $h(x,y)$ 显然无次数大于零的公因元。按照贝朱定理，$h(x,y)=0$ 定义的曲线与此椭圆只有有限个交点。于是，我们可以在椭圆上取一个交点之外的点 (a_1,b_1)。如此，则有

$$a_1^2+a^2b_1^2-1=0,\qquad h(a_1,b_1)=f(a_1,b_1)-g(a_1,b_1)\neq 0.$$

这与原来的假设不合，所以必然有

$$h(x,y)=f(x,y)-g(x,y)\in I.$$

综上所述，我们有

$f(x,y)$，$g(x,y)$ 在椭圆上各点的值皆相等

$\iff f(x,y)-g(x,y)\in I$

$\iff f(x,y),g(x,y)$ 在商环 $\boldsymbol{R}[x,y]/I$ 中的同一等价子集之中。

所以，我们称 $\boldsymbol{R}[x,y]/I$ 为椭圆上的**代数函数环**。定理3.27证明了此环是一个诺德环。

例15 我们举一些非诺德环的例子。令 $C_{\boldsymbol{R}}$ 为直线 $\boldsymbol{R}$ 上的所有连续函数。在普通的加法与乘法之下，$C_{\boldsymbol{R}}$ 成为一交换环。令

$$I_n=\{f(x):\ f(x)\in C_R, f(i)=0,\ \ \forall i\geq n, i\in \boldsymbol{Z}\}.$$

显然有一永不终止的上升的链：

$$I_1\subsetneqq I_2\subsetneqq\cdots\subsetneqq I_n\subsetneqq I_{n+1}\subsetneqq\cdots.$$

所以 C_R 不是诺德环。

又如，令

$$K[x_1,x_2,\cdots,x_n\cdots]$$

$$=\left\{\sum_{有限}a_{i_1\cdots i_n}^{(j_1\cdots j_n)}x_{j_1}^{i_1}\cdots x_{j_n}^{i_n}:\ a_{i_1\cdots i_n}^{(j_1\cdots j_n)}\in K\right\},$$

即为无限元的多项式环。令 $I_n=(x_1,x_2,\cdots,x_n)$。显然有一永不终止的链

$$I_1\subsetneqq I_2\subsetneqq\cdots\subsetneqq I_n\subsetneqq I_{n+1}\subsetneqq\cdots.$$

所以 $K[x_1,x_2,\cdots,x_n,\cdots]$ 不是诺德环。▌

在证明整数环 $\boldsymbol{Z}$、复整数环 $\boldsymbol{Z}[\mathrm{i}]$ 及一元多项式环 $K[x]$——此处 K 是域——的唯一分解定理时，我们总是先证明 $\boldsymbol{Z}, \boldsymbol{Z}[\mathrm{i}]$ 及 $K[x]$ 是主理想环，然后由此导出唯一分解定理。我们把以前的步骤略加系统化，就可以证明以下的一般性的定理了。

定理3.28 设 R 是一个主理想整环，则 R 是一个唯一分解的整环。

证明 我们先证明分解的存在性。这里我们只用到 R 是一个诺德环——一个主理想整环自然是一个诺德环。任取 R 中一非零非可逆的元素 a。如果 a 不可分解，则 $a=a$ 是 a 的分解式。如果 a 可分解成 $b_1\cdot c_1$，而 b_1 及 c_1 皆非零非可逆，于是有

$$a=b_1c_1,\qquad (a)\subsetneqq(b_1),\qquad (a)\subsetneqq(c_1).$$

如 b_1 及 c_1 皆不可分解，则上式即 a 的分解式。反之，设 b_1 可分解成 $b_2\cdot d_2$，则同样地有

$$b_1=b_2d_2,\qquad (b_1)\subsetneqq(b_2),\qquad (b_1)\subsetneqq(d_2).$$

如此反复推论，逐步分解。如始终不能得到 a 的分解式，则

势必有一永不终止的上升的链

$$(a)\subsetneqq(b_1)\subsetneqq(b_2)\subsetneqq\cdots\subsetneqq(b_n)\subsetneqq\cdots.$$

这与诺德环的性质(定理2.35)相违。以此我们证明了诺德环中的任何非零非可逆的元素皆可分解。

关于分解的唯一性，请读者参考第一章§2，§5及第三章§3的定理3.4，3.10，自行补足。▎

习　题

1. 证明$\boldsymbol{Z}[x]$不是主理想环。

2. 设S是一个整环但不是域，证明$S[x]$不是主理想环。

3. 证明$\boldsymbol{Z}[\mathrm{i}]$是一个主理想环。

4. 证明$\boldsymbol{Z}[\mathrm{i}]$内任一非零素理想都是极大理想。

5. 设$I=\{a+b\mathrm{i}: a,b\in 2\boldsymbol{Z}\}$。证明$\boldsymbol{Z}[\mathrm{i}]/I$有零因子。

6. 设R是闭区间$[a,b]$内全体连续函数关于函数加法、乘法所成的环，c是$[a,b]$中一定点。定义R到$\boldsymbol{R}$的映射

$$\varphi: f(x)\mapsto f(c).$$

证明φ是一个环映射，并证明$R/\ker\varphi$同构于$\boldsymbol{R}$。又设I是R的理想，$I\neq\{0\},R$。则存在$\theta\in[a,b]$，使对一切$f(x)\in I$，有

$$f(\theta)=0.$$

7. 设R是一个交换环，I是R的素理想，令

$$I[x]=\{a_0+a_1x+\cdots+a_nx^n: a_i\in I\}.$$

证明$I[x]$是$R[x]$的素理想。

8. 仿照定理3.26，证明：如果R是诺德环，则形式幂级数环$R[[x]]$也是诺德环。

9. 如果R是诺德环，证明$R[[x_1,\cdots,x_n]]$是一个诺德环。

10. 证明$\boldsymbol{Q}[[x_1,\cdots,x_n,\cdots]]=\bigcup\limits_{i=1}^{\infty}\boldsymbol{Q}[[x_1,\cdots,x_i]]$不是诺德环。

11. 如R是诺德环，I是R的理想，证明R/I也是诺德环。

12. 如R_1,R_2是诺德环，证明$R_1\oplus R_2$也是诺德环。

13. 设R是诺德环且为整环，D是一个分母系，证明R_D也是一个诺德环。

14. 设D是整环R的一个分母系，J是与D不相交的理想中的极大者，即理想$I\supsetneqq J\Rightarrow I\cap D\neq\varnothing$。证明$J$是一个素理想。

15. 证明$\boldsymbol{Z}[x]$的每一个极大理想都可以由两个元素生成。

16. 证明有限整环必是域。

17. 写出$\mathbf{Q}[x]/(x(x+1)(x+2))$的所有的理想。

18. 证明诺德环R的任意非零理想I必然包含有限多个素理想的乘积。

19. 求$\boldsymbol{Z}[x]/(4,x^2)$的基数及所有可逆元素。

20. 令$C([0,1])$是闭区间$[0,1]$上的连续函数环，问它是否为诺德环？

21. 令$R=\{a/b:\ a,b\in\boldsymbol{Z},\ b$不被2或3整除$\}$，问$R$是否为诺德环？

第四章　线性代数

§1　向量空间

我们首先给出向量空间的定义如下：

定义4.1　设K是域。一个非空的集合V，如适合下列条件，则称为K**向量空间**，或简称为向量空间：

1）在V中有加法（“+”），且对加法而言，V是一交换群，令其幺元为0，称为**零向量**；

2）任取$a\in K$，$v\in V$，有一双项运算——通常称为乘法（“·”）——存在，使$a\cdot v\in V$及

$$1\cdot v=v,$$

此处1是K的乘法的幺元（乘法符号“·”经常忽略不写）；

3）这四种运算——域K的加法、乘法，V的加法及K与V之间的乘法——适合结合律及分配律，即对所有的$a,a_1,a_2\in K$，v，$v_1,v_2\in V$，都有

$$(a_1a_2)v=a_1(a_2v),\qquad (a_1+a_2)v=a_1v+a_2v,$$

$$a(v_1+v_2)=av_1+av_2.$$

如果V为K向量空间，则V的元素称为**向量**，K的元素称为**常量**。

例1　取$\boldsymbol{R}\times\boldsymbol{R}=\{(a_1,a_2):\ a_1,a_2\in\boldsymbol{R}\}$。定义

$$(a_1,a_2)+(b_1,b_2)=(a_1+b_1,a_2+b_2),$$

$$c(a_1,a_2)=(ca_1,ca_2),\qquad c\in\boldsymbol{R},$$

则$\boldsymbol{R}\times\boldsymbol{R}$成为$\boldsymbol{R}$向量空间，其零向量是(0,0)。在此向量空间内，加法可以图解如下：在平面上取点(a_1,a_2)，(b_1,b_2)。以箭头连接原点(0,0)及此二点，作一平行四边形如图4.1。连接原点及对

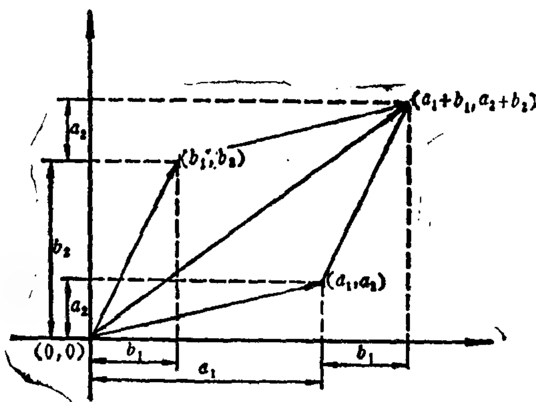


图 4.1

顶点，成一箭头，则箭头的尖点即(a_1+a_2, b_1+b_2)。

同法，我们可以任取一域K，在K的n次直积

$$K^n = K\times K\times\cdots\times K = \{(a_1, a_2, \cdots, a_n):\ a_i\in K\}$$

中定义

$$(a_1,\cdots,a_n)+(b_1,\cdots,b_n)=(a_1+b_1,\cdots,a_n+b_n),$$

$$c(a_1,a_2,\cdots,a_n)=(ca_1,ca_2,\cdots,ca_n)\quad (c\in K),$$

则K^n成为K向量空间，其零向量为$(0,0,\cdots,0)$。

我们也可以取K的可数无限次的直积K^∞，

$$K^\infty = K\times K\times\cdots\times K\times\cdots$$
$$=\{(a_1,a_2,\cdots,a_n,\cdots):\ a_i\in K\}.$$

在其中定义

$$(a_1,\cdots,a_n,\cdots)+(b_1,\cdots,b_n,\cdots)=(a_1+b_1,\cdots,a_n+b_n,\cdots),$$

$$c(a_1,a_2,\cdots,a_n,\cdots)=(ca_1,ca_2,\cdots,ca_n,\cdots)\quad (c\in K),$$

则K^∞成为K向量空间，其零向量为$(0,0,\cdots,0,\cdots)$。

例 2 设环$R\supset$域K。则R自然成为一K向量空间。这因为

环的条件强于向量空间的条件。

于是，多元多项式环$K[x_1,x_2,\cdots,x_n]$是K向量空间。如果域$L\supset$域K，则L是K向量空间。例如，$\mathbf{C}$是$\mathbf{R}$向量空间，$\mathbf{R}$是$\mathbf{Q}$向量空间。

例 3 取一个n元的齐次线性方程组如下：

$$\begin{cases} a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n=0, \\ a_{21}x_1+a_{22}x_2+\cdots+a_{2n}x_n=0, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n1}x_1+a_{n2}x_2+\cdots+a_{nn}x_n=0, \end{cases}$$

此处$a_{ij}\in K$(K为域)。令

$$V=\{(a_1,a_2,\cdots,a_n)\in K^n:\ x_1=a_1,\cdots,x_n=a_n \text{ 是上面方程组的解}\},$$

则显然有$V\ni(0,0,\cdots,0)$，于是V是非空集合。易于看出

$$\alpha,\beta\in V\Longrightarrow\alpha+\beta\in V,\quad c\alpha\in V\ \ (c\in K),$$

此处加法与乘法定义同于K^n。不难看出，V是K向量空间。

例 4 取一个齐次常微分方程如下：

$$\sum_{i=0}^{n}a_i\frac{d^if(x)}{dx^i}=\left(\sum_{i=0}^{n}a_i\frac{d^i}{dx^i}\right)f(x)=L(D)f(x)=0,$$

此处$a_i\in\mathbf{R}$，$f(x)$是n次可微实函数。令

$$V=\{f(x):\ L(D)f(x)=0,\ f(x)\text{是}n\text{次可微函数}\}.$$

则有$0\in V$。于是V是非空集合。在V中定义加法如同一般函数的加法，定义实数c与函数$f(x)$的乘法也如同一般的乘法。不难看出，V是$\mathbf{R}$向量空间。▎

线性代数的起源是解线性联立方程组——齐次的或非齐次的。古中国的数学书《九章算术》（公元一世纪以前）开创了线性代数的先河。这本书的方法是把n元线性联立方程组的系数a_{ij}取出，排成一个“方程”，也即现代所谓的“矩阵”。《九章算术》的数学术语一直影响到现代：含有变数的数学等式被称

为“方程式”，虽然它经常不是“方”的。

从K向量空间的定义里，我们立刻可以导出

$$0\cdot v+0\cdot v=(0+0)v=0\cdot v,$$

故 $$0\cdot v=(0\cdot v+0\cdot v)-0\cdot v=0\cdot v-0\cdot v=0,$$

以及 $$(-a)v+av=(-a+a)v=0\cdot v=0.$$

定义4.2 设U是K向量空间V的子集。如果U对同样的加法及乘法构成K向量空间，则称U为V的**子空间**。设S是V的子集，包含S的V的最小的子空间称为S**生成的子空间**，记为$\langle S\rangle$。S称为$\langle S\rangle$的**生成子集**或**生成元集**。

讨论 如S是空集时，$\langle S\rangle$自然是零空间$\{0\}$，其中仅有零向量。如S不是空集时，我们可以证明

$$\langle S\rangle=\left\{\sum_{\text{有限}}a_iv_i:\ a_i\in K,\ v_i\in S\right\}.$$

事实上，令上式右侧为U，不难看出，U确为一包含S的子空间。于是，要证明上式，仅须证明任一包含S的子空间必定包含U。如此，U自然是包含S的最小的子空间了。设U^*是包含S的一个子空间，则有

$$\begin{aligned}S\subset U^*&\Longrightarrow v_i\in U^*,\ \ \forall v_i\in S\\&\Longrightarrow a_iv_i\in U^*,\ \ \forall a_i\in K,\ v_i\in S\\&\Longrightarrow\sum_{\text{有限}}a_iv_i\in U^*,\ \ \forall a_i\in K,\ v_i\in S\\&\Longrightarrow U\subset U^*.\end{aligned}$$

习 题

1. 证明$\mathrm{FL}(n,\boldsymbol{R})$是$\boldsymbol{R}$向量空间。

2. 证明域K上的所有次数不超过n的一元多项式构成向量空间。

3. 证明$[0,1]$上所有连续函数构成$\boldsymbol{R}$向量空间。

4. 证明[0,1]上无限可微函数的集合 $C^\infty([0,1])$ 构成 $\boldsymbol{R}$ 向量空间。

5. 设 V 是向量空间，$V_1,\cdots,V_n$ 是 V 的子空间。定义 $V_1,\cdots,V_n$ 的和为

$$V_1+\cdots+V_n=\{a_1+\cdots+a_n:\ a_i\in V_i(i=1,\cdots,n)\}.$$

证明 $V_1+\cdots+V_n$ 是 V 的子空间。

6. $\mathrm{FL}(n,\boldsymbol{R})$ 中所有第 i 列($1\leqslant i\leqslant n$)为零的矩阵的集合构成子空间，以 V_i 表示之。证明

$$\mathrm{FL}(n,\boldsymbol{R})=V_i+V_j\quad(i\neq j).$$

7. 设 V 为向量空间，$V_1,V_2,\cdots,V_n$ 为子空间。如果 $V=V_1+V_2+\cdots+V_n$，且 V 中任一元素 a 能唯一地表成 $a=a_1+a_2+\cdots+a_n(a_i\in V_i)$，则称 V 是 $V_1,V_2,\cdots,V_n$ 的直和，记为 $V=V_1\oplus V_2\oplus\cdots\oplus V_n$（这样的 $V_1,\cdots,V_n$ 称为 V 的直和因子）。证明下述三条是等价的：

(1) $V=V_1\oplus V_2\oplus\cdots\oplus V_n$；

(2) $V=V_1+V_2+\cdots+V_n$，且 $a_1+a_2+\cdots+a_n=0\ (a_i\in V_i)\Longrightarrow a_i=0(\forall i=1,2,\cdots,n)$，亦即 0 只能唯一地表成 $V_i(i=1,2,\cdots,n)$ 中元素之和；

(3) $V=V_1+V_2+\cdots+V_n$，且

$$V_i\cap\Big(\sum_{j\neq i}V_j\Big)=\{0\}\quad(\forall i=1,2,\cdots,n).$$

8. 在通常的三度空间中取定一直角坐标系。空间中的点的加法以及实数与点的乘法如常，则得到一个向量空间。证明过原点的任一直线以及平面都是子空间；反之，任一非平凡的子空间必然是过原点的直线或平面。试刻画三度空间的直和因子之间的关系。

9. 将本节习题 2 中的 V 表成 j 个子空间的直和（$j=2,3,\cdots,n$）。

10. 证明 $\boldsymbol{R}$ 向量空间 $\mathrm{FL}(n,\boldsymbol{R})$不能表成 n^2+1个子空间的直和。

11. 设 V 是由 n 个向量生成的向量空间。证明 V 不能表成多于 n 个子空间的直和。

12. 设 $V=V_1\oplus V_2\oplus\cdots\oplus V_n$。证明 $V_1+V_2+\cdots+V_{n-1}\neq V$。若有子空间 $U_1\subsetneqq V_1$，证明 $U_1+V_2+\cdots+V_n$不是直和。设 U 是任一非零子空间，证明 $V_1+V_2+\cdots+V_n+U$ 不是直和。

13. 令

$$V=\left\{(a_1,a_2,\cdots,a_n):\ a_i\in\boldsymbol{R}(i=1,2,\cdots,n),\ \sum_{i=1}^{n}a_i=0\right\},$$

$$W=\{(a,a,\cdots,a):\ a\in\boldsymbol{R}\}.$$

证明 $\boldsymbol{R}^n=V\oplus W$。试解释其几何意义。

14. 设 V 是向量空间，U,W 是其子空间。如果 $V=U\cup W$，证明

$$V=U\quad 或\quad V=W。$$

15. 证明无限域上的向量空间不能表成有限多个真子空间的并集。

§2 基及维数

设 V 是一个 K 向量空间，我们自然有 $\langle V\rangle=V$，也即 V 是 V 的生成元集。所以生成元集是存在的。

定义4.3 设 S 是一个 K 向量空间 V 的极小的生成元集，即 S 适合下列两条件：

1） S 是 V 的生成元集：$\langle S\rangle=V$；

2） 任取 $v\in S$，则恒有 $\langle S\setminus\{v\}\rangle\neq V$。即从 S 中去掉任何一个元素 v，则余下的集合不构成 V 的生成元集，则称 S 是 V 的一组基。

定义4.4 设S是K向量空间V的一个子集。如果S适合下列条件，则称S为**线性无关集**：任取有限个$a_i \in K$，$v_i \in S$，则$\sum_i a_i v_i = 0$时，必有$a_i = 0$，$\forall i$。

定理4.1 设S是K向量空间V的子集，则下列的三条件是同等的，因此都可作为基的定义：

1）S是极小的生成元集；

2）S是极大的线性无关集；

3）S是线性无关的生成元集。

证明 1）$\Longrightarrow$ 2）。设S是V的极小生成元集。如有

$$a_1 v_1 + a_2 v_2 + \cdots + a_n v_n = 0,$$

其中$v_i \in S$，a_i不全为零。不妨即令$a_1 \neq 0$。上式乘以a_1^{-1}，令$-b_i = a_i a_1^{-1}$，则得下式：

$$v_1 - b_2 v_2 - b_3 v_3 - \cdots - b_n v_n = 0,$$

即
$$v_1 = b_2 v_2 + b_3 v_3 + \cdots + b_n v_n.$$

我们将证明$S \setminus \{v_1\}$也是V的生成元集，如此，则S不是V的极小生成元集，这是一个矛盾。于是知道S是一个线性无关集。

任取$v \in \langle S \rangle$，则有

$$v = \sum_{\text{有限}} c_j u_j, \qquad c_j \in K, \ u_j \in S.$$

如果上式的u_j皆与v_1不同，则自然皆在$S \setminus \{v_1\}$中。于是有$v \in \langle S \setminus \{v_1\} \rangle$。如果有一$u_j$与$v_1$相同，不妨即令$u_1 = v_1$。于是

$$v = c_1 u_1 + \sum_{j \neq 1} c_j u_j = c_1 (b_2 v_2 + \cdots + b_n v_n) + \sum_{j \neq 1} c_j u_j.$$

此式右侧的v_i及u_j皆在$S \setminus \{v_1\}$中，所以仍有

$$v \in \langle S \setminus \{v_1\} \rangle.$$

这就证明了$S \setminus \{v_1\}$是V的生成元集。这个矛盾现象，说明了S必然是线性无关集。

其次，我们要证明S是"极大"的线性无关集．对于任一$v\in V\backslash S$．因为S是V的生成元集，所以$v\in\langle S\rangle$，即存在有限个$r_i\in K$，使

$$v=\sum_i r_i v_i,\qquad v_i\in S.$$

即

$$(-1)v-\sum_i r_i v_i=0,\qquad v,v_i\in S\cup\{v\}.$$

上式的首项系数$-1\neq 0$，由此证明了$S\cup\{v\}$不是线性无关集．

2）$\Longrightarrow$1）．设S是一个极大的线性无关集．我们首先要证明S是v的生成元集．任取$v\in V\backslash S$，则$S\cup\{v\}$不是线性无关集．所以有

$$av+\sum_{\text{有限}} a_i v_i\neq 0,\qquad a,a_i(\in K)\text{不全为零},\ v_i\in S.$$

在上式中，必然有$a\neq 0$．否则此式可以写成

$$\sum a_i v_i=0,\qquad a_i(\in K)\text{不全为零},\ v_i\in S.$$

这与S是线性无关集的假设不合．令$b_i=-a_i a^{-1}$，则有

$$v=\sum_i b_i v_i,\qquad v_i\in S.$$

即$v\in\langle S\rangle$．于是S是V的生成元集．

如果S不是极小的生成元集，我们将引出一矛盾如下：此时必有一$v\in S$，使$\langle S\backslash\{v\}\rangle=V$．特别是$v\in V$，于是有下式：

$$v=\sum_{\text{有限}} a_i v_i,\qquad a_i\in K,\ v_i\in S\backslash\{v\}.$$

移项后，有

$$(-1)v+\sum_{\text{有限}} a_i v_i=0,\qquad v,v_i\in S.$$

在上式中，v的系数$-1\neq 0$，这意味着S不是线性无关集．这是

矛盾的。所以S是极小的生成元集。

1)，2)$\Longrightarrow$3)．显然．3)$\Longrightarrow$1)．读者自证．∎

以下，我们要用第一章§1的“Zorn引理”来证明基的存在性。

定理4.2 设V是一个K向量空间，则V有一组基。

证明 如果V是零向量空间$\{0\}$，则空集是V的基。一般情形时，取$\mathscr{F}$如下：

$$\mathscr{F}=\{S: S\text{是}V\text{中的线性无关集}\}.$$

空集$\varnothing\in\mathscr{F}$，所以$\mathscr{F}$非空。证明$\mathscr{F}$非空的另一法如下：已设$V\neq\{0\}$，任取$v\in V\setminus\{0\}$，即$v\neq 0$，我们可证$\{v\}\in\mathscr{F}$。事实上，假若$\{v\}$不是线无关集，则存在$0\neq a\in K$，使

$$av=0.$$

乘以a^{-1}，得

$$v=(a^{-1}a)v=a^{-1}(av)=a^{-1}\cdot 0=0,$$

这是一个矛盾。所以$\{v\}\in\mathscr{F}$，也即$\mathscr{F}$是非空的。

在$\mathscr{F}$中定义半序“$\leqslant$”如下：

$$S_1\leqslant S_2 \iff S_1\subset S_2.$$

任取一链$\mathscr{G}\subset\mathscr{F}$．令

$$S=\bigcup S_i,\quad S_i\in\mathscr{G}.$$

则显然有

$$S\geqslant S_i,\quad \forall S_i\in\mathscr{G}.$$

我们要证明$S\in\mathscr{F}$．如此，则S是$\mathscr{G}$的上限．设S不是线性无关集，则存在不全为零的a_j，使

$$\sum_{\text{有限}}a_jv_j=0,\quad a_j\in K,\ v_j\in S=\bigcup S_i.$$

令

$$v_j\in S_{n_j}\in\mathscr{G}.$$

因为$\mathscr{G}$是一链，故有限个S_{n_j}中必有某个S_{n_j}包含其余的．不妨

令此为$S_l\in\mathscr{G}\subset\mathscr{F}$。于是有

$$\sum_j a_j v_j=0,\qquad a_j\in K\text{ 不全为零},\ v_j\in S_l\in\mathscr{F}.$$

此是一矛盾。故得$S\in\mathscr{F}$。

我们验证了Zorn引理的条件。于是根据Zorn引理的结论，$\mathscr{F}$中至少有一极大的线性无关集S。由定理4.1，此S必然是V的基。∎

下面这个引理将要用于建立向量空间的“维数”的概念。

引理 给定一个向量空间V，一个生成元集S及一个线性无关集S'。则我们恒有

$$S\text{ 的基数}\geqslant S'\text{ 的基数。}$$

证明 我们用Zorn引理。考虑如下的集合

$$\mathscr{F}=\{(T,\rho,T'):\ T\subset S,\ T'\subset S',\ \rho\text{是自}T\text{到}T'\text{的单满映射},\ T\cap(S'\backslash T')=\text{空集},\ T\cup(S'\backslash T')\text{是线性无关集}\}.$$

这个集合$\mathscr{F}$的元素(T,ρ,T')可以理解成用S的子集T来替换S'的子集T'，ρ的作用是保证T与T'的基数相同。要证明本引理，无非是要证明$\mathscr{F}$中有一元素(T,ρ,S')，如此，则S'与S的一个子集T同基数，而这恰是集合论中下列不等式的定义：

$$S\text{ 的基数}\geqslant S'\text{ 的基数。}$$

我们首先要验证Zorn引理的条件。令$T=$空集，$T'=$空集，$\rho=$空映射，则自然有$(T,\rho,T')\in\mathscr{F}$，故$\mathscr{F}$不是空集。

在$\mathscr{F}$中定义半序“$\leqslant$”如下：

$$(T_1,\rho_1,T'_1)\leqslant(T_2,\rho_2,T'_2)$$
$$\Longleftrightarrow T_1\subset T_2,\ T'_1\subset T'_2,\ \text{且}\ \rho_2(t)=\rho_1(t),\ \forall t\in T_1.$$

不难看出，“$\leqslant$”符合半序的定义。在$\mathscr{F}$中任取一链$\{(T_i,\rho_i,T'_i)\}$。我们要证明此链在$\mathscr{F}$中有上限。令$T=\bigcup T_i,T'=\bigcup T'_i$，$\rho$的定义如下：

$$\rho(t)=\rho_i(t),\qquad t\in T_i.$$

如能证明(T,ρ,T')在$\mathscr{F}$中，则它自然是该链的上限。

不难看出，$T\subset S$，$T'\subset S'$，ρ是由T到T'的单满映射。我们来证明$T\cap(S'\backslash T')$是空集。如果$t\in T\cap(S'\backslash T')$，则$t\in T=\bigcup T_i$。于是存在一确定的$i$，使$t\in T_i$。然而

$$S'\backslash T'\subset S'\backslash T'_i,$$

于是$t\in T_i\cap(S'\backslash T'_i)=$空集。这是不可能的。所以$T\cap(S'\backslash T')$是空集。其次，我们要证明$T\cup(S'\backslash T')$是线性无关集。任取有限个$t_1,t_2,\cdots,t_n\in T\cup(S'\backslash T')$。不妨设$t_1,t_2,\cdots,t_l\in T$，$t_{l+1},\cdots,t_n\in(S'\backslash T')$。于是，适当地选取$m_j(j=1,2,\cdots,l)$后，有

$$t_1\in T_{m_1},\qquad t_2\in T_{m_2},\ \cdots,\ t_l\in T_{m_l}.$$

因为$\{(T_i,\rho,T'_i)\}$是一链，所以有一r，使得

$$T_{m_1}\subset T_r,\ T_{m_2}\subset T_r,\ \cdots,\ T_{m_l}\subset T_r.$$

如上证明，我们有

$$S'\backslash T'\subset S'\backslash T'_r,$$

所以得出

$$t_1,t_2,\cdots,t_l,t_{l+1},\cdots,t_n\in T_r\cup(S'\backslash T'_r).$$

但是$T_r\cup(S'\backslash T'_r)$是线性无关集，所以$t_1,t_2,\cdots,t_n$线性无关。于是$T\cup(S\backslash T')$是线性无关集。我们完满地证明了$(T,\rho,T')\in\mathscr{F}$。

以上验证了Zorn引理的条件。根据Zorn引理，$\mathscr{F}$中有一极大元素$(\bar{T},\bar{\rho},\bar{T}')$。我们只要证明$\bar{T}'=S'$成立，则本引理即得证。

假设$\bar{T}'\neq S'$，即$S'\backslash\bar{T}'$是非空的。令$s'\in S'\backslash\bar{T}'$。因为$\bar{T}\cup(S'\backslash\bar{T}')$是线性无关集，所以

$$s'\,\overline{\in}\,\langle\bar{T}\rangle=\bar{T}\text{生成的子空间},$$

故

$$\langle\bar{T}\rangle\neq V=\langle S\rangle.$$

于是S中至少有一元素s，使

$$s\overline{\in}\langle \boldsymbol{T}\rangle,$$

即$\{s\}\cup \boldsymbol{T}$为线性无关集。我们考虑两种可能：

1) $s\overline{\in}\langle \boldsymbol{T}\cup(S'\backslash \boldsymbol{T}')\rangle$；

2) $s\in\langle \boldsymbol{T}\cup(S'\backslash \boldsymbol{T}')\rangle$。

在1)的情形下，令$T^*=\{s\}\cup \boldsymbol{T}$，$(T^*)'=\{s\}\cup \boldsymbol{T}'$，$\rho^*$定义如下：

$$\rho^*(t)=\bar{\rho}(t),\qquad 如果t\neq s,$$

$$\rho^*(s)=s'.$$

则不难看出$(T^*,\rho^*,(T^*)')\in\mathscr{F}$，而且有

$$(\boldsymbol{T},\bar{\rho},\boldsymbol{T}')<(T^*,\rho^*,(T^*)').$$

此与$(\boldsymbol{T},\bar{\rho},\boldsymbol{T}')$是极大元素相矛盾，这是不可能的。

在情形2)下，s可以表成$\boldsymbol{T}\cup(S'\backslash \boldsymbol{T}')$中有限多个元素的线性组合，即

$$(1)\qquad s=\sum_i a_it_i+\sum_j b_jt_j',\qquad t_i\in \boldsymbol{T},\ t_j'\in S'\backslash \boldsymbol{T}'.$$

其中a_i,b_j显然不全为零。进而言之，如果b_j全为零，则与$\{s\}\cup \boldsymbol{T}$为线性无关集矛盾。所以至少有一个b_j不为零，不妨即令$b_1\neq 0$。于是我们令$T^*=\{s\}\cup \boldsymbol{T}$，$(T^*)'=\{t_1'\}\cup \boldsymbol{T}'$，再定义$\rho^*$如下：

$$\rho^*(t)=\bar{\rho}(t),\qquad 如果t\neq s,$$

$$\rho^*(s)=t_1'.$$

我们要证明$(T^*,\rho^*,(T^*)')\in\mathscr{F}$。以下仅证明$T^*\cup(S'\backslash(T^*)')$是线性无关集，读者自证其余各点。

设有一个线性方程式如下，其中系数α,α_i,β_j不全为零：

$$(2)\qquad \alpha s+\sum_i \alpha_it_i+\sum_{j\neq 1}\beta_jt_j'=0,\qquad t_i\in \boldsymbol{T},\ t_j'\in S'\backslash(T^*)'.$$

由$\boldsymbol{T}\cup(S'\backslash \boldsymbol{T}')$是线性无关集，可知$\alpha\neq 0$。然后由(1)，(2)两式，得

$$\sum_{i} (aa_i + \alpha_i)t_i + ab_1t'_1 + \sum_{j \neq 1} (ab_j - \beta_j)t_j = 0.$$

在此式中$ab_1 \neq 0$，而 $t_i, t'_1, t'_j \in T \cup (S' \backslash T')$。但$T \cup (S' \backslash T')$是线性无关集，这样，得出一个矛盾。于是，不可能有(2)式存在，也即 $T^* \cup (S' \backslash (T^*)')$是线性无关集。

显然，我们有

$$(T, \rho, T') < (T^*, \rho^*, (T^*)'),$$

此与(T, ρ, T')是极大元素的事实相矛盾。

综上所述，$T' = S'$。 ▎

如果在向量空间V中，任取两组基S及S'。则根据上面的引理，我们得出

$$S\text{的基数} \geqslant S'\text{的基数},$$

$$S'\text{的基数} \geqslant S\text{的基数}.$$

根据集合论中基数的大小的比较法则(参考豪斯道夫的《集论》)，有

$$S\text{的基数} = S'\text{的基数}.$$

于是我们有

定理4.3 K向量空间V的任意两组基都有相同的基数。这个共同的基数称为V的维数，用符号 $\dim_k V$或 $\dim V$ 表示之。 ▎

例5 令

$$P_n(\boldsymbol{R}) = \{f(x): f(x) \in \boldsymbol{R}[x], \deg f(x) \leqslant n\}.$$

不难看出$\{1, x, \cdots, x^n\}$是$P_n(\boldsymbol{R})$的基。于是，我们有

$$\dim P_n(\boldsymbol{R}) = n + 1.$$

我们令

$$f_m(x) = \frac{1}{m!} x(x-1)\cdots(x-m+1).$$

则有

$$\deg f_m(x) = m.$$

不难看出 $\{f_0 = 1, f_1, f_2, \cdots, f_n\}$ 也是 $P_n(\boldsymbol{R})$的基。这是郭守敬在

《授时历》(1280年)中首先使用的一组基。这组基的方便之处可以叙明如下。为简明起见，不妨令$n=3$。任取$f(x)\in P_3(\boldsymbol{R})$，其展开式是

$$f(x)=a_0+a_1x+a_2\left(\frac{1}{2!}x(x-1)\right)+a_3\left(\frac{1}{3!}x(x-1)(x-2)\right).$$

在测定这个多项式的系数时(例如每日午夜，观测某种天象)可取$x=0,1,2,3$。则数据$f(0),f(1),f(2),f(3)$应有下列关系

$$f(0)=a_0,\qquad f(1)=a_0+a_1,$$

$$f(2)=a_0+2a_1+a_2,\qquad f(3)=a_0+3a_1+3a_2+a_3.$$

细心的读者可以注意到，上列的系数即“二项展开式”的系数。定义一阶差分$\Delta_1(x)$如下：

$$\Delta_1(0)=f(1)-f(0)=a_1,$$

$$\Delta_1(1)=f(2)-f(1)=a_1+a_2,$$

$$\Delta_1(2)=f(3)-f(2)=a_1+2a_2+a_3.$$

所得的系数又是“二项展开式”的系数。定义二阶差分$\Delta_2(x)$如下：

$$\Delta_2(0)=\Delta_1(1)-\Delta_1(0)=a_2,$$

$$\Delta_2(1)=\Delta_1(2)-\Delta_1(1)=a_2+a_3.$$

同法定义三阶差分$\Delta_3(x)$如下：

$$\Delta_3(0)=\Delta_2(1)-\Delta_2(0)=a_3.$$

于是我们有下列展开式：

$$f(x)=f(0)+\Delta_1(0)x+\Delta_2(0)\left(\frac{1}{2!}x(x-1)\right)$$

$$+\Delta_3(0)\left(\frac{1}{3!}x(x-1)(x-2)\right).$$

上面这个方法的好处是仅须把各点的函数值迭次相减，便可得到函数$f(x)$的各项系数。

对于维数，我们有下面关于几何性质的定理。这里仅证明有限维数的情形。

定理4.4 设U及W是一有限维数的向量空间V的子空间。我们恒有

$$\dim U+\dim W=\dim\langle U\cup W\rangle+\dim(U\cap W).$$

证明 不妨即令$\langle U\cup W\rangle=V$。显然的，$U\cap W$也是V的子空间。取$U\cap W$的一组基$\{v_1,\cdots,v_l\}$。在U及W中分别将$\{v_1,\cdots,v_l\}$扩充成极大的线性无关集，如此成为U及W的基如下：

$$\{v_1,\cdots,v_l,u_{l+1},\cdots,u_n\}\text{是}U\text{的基},$$

$$\{v_1,\cdots,v_l,w_{l+1},\cdots,w_m\}\text{是}W\text{的基}.$$

我们将证明$\{v_1,\cdots,v_l,u_{l+1},\cdots,u_n,w_{l+1},\cdots,w_m\}$是$V$的基，如此，则得出

$$\begin{aligned}\dim U+\dim W&=n+m=(n+m-l)+l\\&=\dim V+\dim(U\cap W)\\&=\dim\langle U\cup W\rangle+\dim(U\cap W).\end{aligned}$$

我们先证这是线性无关集。设有线性方程式如下：

$$\sum_i a_iv_i+\sum_j b_ju_j+\sum_k c_kw_k=0.$$

令

$$v=\sum_i a_iv_i+\sum_j b_ju_j=-\sum_k c_kw_k,$$

则$v\in U\cap W$。故v可以写成$\sum_i d_iv_i$。代入上式，得

$$\sum_i d_iv_i+\sum_k c_kw_k=0.$$

因为$\{v_i,w_k\}$是W的基，所以

$$d_i=0,\qquad c_k=0,\qquad \forall d_i,c_k.$$

故

$$\sum_i a_iv_i+\sum_j b_ju_j=-\sum_k c_kw_k=0,$$

又因为$\{v_i,u_j\}$是U的基，所以

$$a_i=0,\qquad b_j=0,\qquad \forall a_i,b_j.$$

如此我们证明了 $\{v_1,\cdots,v_l,u_{l+1},\cdots,u_n,w_{l+1},\cdots,w_m\}$ 是一个线性无关集。

其次，我们要证明这是一个极大的线性无关集。任取 $v\in V=\langle U\cup W\rangle$，则有

$$v=\sum_i \alpha_i^* u_i^*+\sum_j \beta_j^* w_j^*,\qquad u_i^*\in U,\ w_j^*\in W.$$

把 u_i^* 及 w_j^* 表成给定的两组基的展开式，代入上式，得

$$v=\sum_i \alpha_i v_i+\sum_j \beta_j u_j+\sum_k \gamma_k w_k.$$

这说明 $\{v,v_1,\cdots,v_l,u_{l+1},\cdots,u_n,w_{l+1},\cdots,w_m\}$ 是线性相关集。故 $\{v_1,\cdots,v_l,u_{l+1},\cdots,u_n,w_{l+1},\cdots,w_m\}$ 是极大的线性无关集，即是 V 的基。▎

习　题

1. 视 $K[x]$ 为域 K 上的向量空间。设有 $f_i(x)\in K[x]$ $(i=1,2,\cdots,n)$，且 $\deg f_i$ 两两不同，证明 $f_1,f_2,\cdots,f_n$ 线性无关。

2. 在上题中将deg换成 ord，证明同样的结论。

3. 设 $a,b,c\in \boldsymbol{C}$。三向量 $(1,a,a^2),(1,b,b^2),(1,c,c^2)$ 线性无关的充要条件是什么？

4. 找出 $\boldsymbol{R}^3$ 中四个向量 $(1,2,3),(4,5,6),(7,8,9),(10,11,12)$ 中的所有极大线性无关组。

5. 令

$$V=\left\{(a_1,a_2,\cdots,a_n):\ a_i\in \boldsymbol{R},\ \sum_{i=1}^{n} a_i=0\right\}.$$

找出 V 的一组 $\boldsymbol{R}$ 基。

6. 令 $F=\boldsymbol{Z}/2\boldsymbol{Z}$（两个元素构成的域），$V$ 是一个四维 F 向量空间。V 中有多少元素？V 有几组不同的基？

7. 设 K 为无限域，V 为 K 向量空间。证明 V 有无穷多组不同的基。

8. 设V是K向量空间，$\{\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n\}$为$V$的一组基。令

$$(*)\quad\begin{cases}\xi_1=a_{11}\varepsilon_1+a_{21}\varepsilon_2+\cdots+a_{n1}\varepsilon_n,\\ \xi_2=a_{12}\varepsilon_1+a_{22}\varepsilon_2+\cdots+a_{n2}\varepsilon_n,\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ \xi_n=a_{1n}\varepsilon_1+a_{2n}\varepsilon_2+\cdots+a_{nn}\varepsilon_n,\end{cases}\quad a_{ij}\in K.$$

证明$\{\xi_1,\xi_2,\cdots,\xi_n\}$是$V$的基$\Longleftrightarrow$(*)式右端系数行列式$\neq 0$。

9. 设有R^3中的六个向量$\varepsilon_1=(1,0,0)$，$\varepsilon_2=(0,1,0)$，$\varepsilon_3=(0,0,1)$，$\xi_1=(-1,1,1)$，$\xi_2=(1,-1,1)$，$\xi_3=(1,1,-1)$。

(1) 证明$\{\xi_1,\xi_2,\xi_3\}$是一组基；

(2) 将$\varepsilon_1,\varepsilon_2,\varepsilon_3$表成$\xi_1,\xi_2,\xi_3$的线性组合；

(3) 将$x_1\varepsilon_1+x_2\varepsilon_2+x_3\varepsilon_3$表成$\xi_1,\xi_2,\xi_3$的线性组合(这里$x_1,x_2,x_3\in R$)，进而总结出坐标变换公式。

10. 设V是向量空间，U,W是V的子空间。证明

$U+W$是直和$\Longleftrightarrow \dim(U+W)=\dim U+\dim W$。

11. 求元素取自C的所有$n\times n$对称矩阵所构成的C向量空间V的维数及元素在C中的所有$n\times n$反对称矩阵所构成的C向量空间W的维数。证明$FL(n,C)=V\oplus W$。

12. 设

$$U=\{(a_1,a_2,\cdots,a_{2n})\in C^{2n}:\ a_1=a_2=\cdots=a_n=0\},$$

$$W=\{(a_1,a_2,\cdots,a_{2n})\in C^{2n}:\ a_j=a_{n+j}(\forall j=1,2,\cdots,n)\}.$$

证明U和W都是C^{2n}的子空间，且$C^{2n}=U\oplus W$。

13. 设V为向量空间，且$V=V_1\oplus V_2\oplus\cdots\oplus V_r$。证明$V_1,V_2,\cdots,V_r$的基的并集是$V$的一组基。

§3 线性变换及矩阵

代数学的中心题材之一是研究各代数实体间的关系。在线性代数的范围内，我们要研究向量空间的线性变换。其定义如下：

定义4.5 设T是自K向量空间V到K向量空间W的一个映射，此处K是一域。如果T适合下列条件，则称T是一个K**线性变换**(或简称线性变换)：

1) $T(v_1+v_2)=T(v_1)+T(v_2)$，$\forall v_1,v_2\in V$，

2) $T(av)=aT(v)$，$\forall a\in K$，$v\in V$。

例 6 设$V=\boldsymbol{R}^3,W=\boldsymbol{R}^2$，$T(a_1,a_2,a_3)=(a_1,a_2)$。不难看出，$T$是一个线性变换。这是从三维空间$\boldsymbol{R}^3$到平面$\boldsymbol{R}^2$的投影。

设$V=W=\boldsymbol{R}^2$，T是以原点为旋转心，旋转角为θ的旋转。不难看出T是一个线性变换。

设$V=W=C^\infty(\boldsymbol{R})$，即一元无限次可微实函数集合。令$D$为微分算子，即$\mathrm{d}/\mathrm{d}x$，其作用如下：

$$D(f(x))=\frac{\mathrm{d}f(x)}{\mathrm{d}x}=f'(x),$$

则D是一个线性变换。

设$V=W=C(\boldsymbol{R})$，即一元连续实函数集合。令$\int$为上限不定的积分(不妨定其下限为零)，即

$$\int(f(x))=\int_0^x f(x)\mathrm{d}x,$$

则$\int$是一个线性变换。

例 7 解多元联立一次方程组，可以理解成线性变换的问题。我们取三元联立一次方程组为例，

$$\begin{cases}a_{11}x_1+a_{12}x_2+a_{13}x_3=b_1,\\ a_{21}x_1+a_{22}x_2+a_{23}x_3=b_2,\\ a_{31}x_1+a_{32}x_2+a_{33}x_3=b_3.\end{cases}$$

这组方程式的系数a_{ij}决定一个线性变换A: $\boldsymbol{R}^3\to\boldsymbol{R}^3$。我们把$\boldsymbol{R}^3$中的向量写成三行一列的矩阵

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix},$$

令

$$A\left(\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}\right)=\begin{bmatrix} a_{11}x_1+a_{12}x_2+a_{13}x_3 \\ a_{21}x_1+a_{22}x_2+a_{23}x_3 \\ a_{31}x_1+a_{32}x_2+a_{33}x_3 \end{bmatrix}.$$

于是，原线性方程组可以写成下式：

$$A\left(\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}\right)=\begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}.$$

如此，则有

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}\in A^{-1}\left(\begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}\right)=\begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}\text{的象源.}$$

如果此象源为非空的，则原方程组有解。▌

给定K向量空间V及W。考虑所有自V到W的线性变换的集合，以$\mathrm{Hom}_K(V,W)$表示之。在此集合内，我们可以引入一种自然的K向量空间的结构如下：

设$T_1,T_2,T\in\mathrm{Hom}_K(V,W)$，$a\in K$，定义

$$(T_1+T_2)(v)=T_1(v)+T_2(v),\qquad \forall v\in V,$$

$$(aT)(v)=aT(v),\qquad \forall v\in V.$$

不难看出，$\mathrm{Hom}_K(V,W)$成为K向量空间。

如果$V=W$，我们在$\mathrm{Hom}_K(V,V)$中，尚可引入一个乘法如下：

$$(T_1\circ T_2)(v)=T_1(T_2(v)),$$

其中$T_1,T_2\in\mathrm{Hom}_K(V,V)$，$v\in V$。对于此乘法，如下定义的幺线性变换$I$

$$I(v)=v,\qquad \forall v\in V$$

自然是乘法的幺元。不难看出，$\mathrm{Hom}_K(V,V)$成为一环。综上所

述，我们有：

定理 4.5 $\mathrm{Hom}_K(V,W)$是K向量空间，$\mathrm{Hom}_K(V,V)$是环. ▌

我们任取V的一组基$\{v_i\}$及W的一组基$\{w_j\}$。定义线性变换Δ_j^i如下：

$$\Delta_j^i(v_s)=\delta_s^i w_j,$$

其中

$$\delta_s^i=\begin{cases}1, & \text{如果 } i=s,\\ 0, & \text{如果 } i\neq s.\end{cases}$$

定理 4.6 如果$\dim V=n<\infty$，$\dim W=m<\infty$，则$\{\Delta_j^i\}$是$\mathrm{Hom}_K(V,W)$的一组基。于是

$$\dim \mathrm{Hom}_K(V,W)=(\dim V)(\dim W)=nm.$$

证明 1）我们首先证明$\{\Delta_j^i\}$是线性无关集。设有一线性方程式如下：

$$\sum_{i,j}a_{ij}\Delta_j^i=0,$$

其中0表示零线性变换。则对任意的s，有

$$\sum_{i,j}a_{ij}\Delta_j^i(v_s)=\sum_j a_{sj}w_j=0.$$

因为$\{w_j\}$是基，所以得出

$$a_{sj}=0,\qquad \forall s,j.$$

2）我们要证明$\{\Delta_j^i\}$是一个生成元集。任取$T\in\mathrm{Hom}_K(V,W)$，设$T(v_s)=\sum_j b_{sj}w_j$。取T'如下：

$$T'=T-\sum_{i,j}b_{ij}\Delta_j^i.$$

立得

$$T'(v_s)=T(v_s)-\sum_{i,j}b_{ij}\Delta_j^i(v_s)$$

$$= \sum_j b_{sj} w_j - \sum_j b_{ij} w_j = 0.$$

任取 $v = \sum c_s v_s$，则有 $T'(v) = \sum_s c_s T'(v_s) = 0$。所以

$$T - \sum_{i,j} b_{ij} \Delta_j^i = 0.$$

上式证明了$\{\Delta_j^i\}$是生成元集。根据定理4.1的 3)，即可知 $\{\Delta_j^i\}$ 是 $\mathrm{Hom}_K(V, W)$的一组基。❙

讨论 如果 $V = W$及 $\dim V = \infty$时，$\{\Delta_j^i\}$不是生成元集。例如，乘法的幺元 I 只能写成

$$I = \sum_i \Delta_i^i,$$

而上式取和时有无限多项。在不谈极限概念时，我们不能取无限多项的和；因此上式是没有意义的。❙

从抽象的代数实体，到具体的代数模型，我们需要寻求一种"表示法"或"坐标系"。为此我们引入如下的定义。

定义4.6 设 $\rho: V \to W$ 为线性变换。如果 ρ 为满单映射时，则称ρ为**同构**。如果ρ为同构，且 $W = K^n$，则称ρ为V的一种**表示法**或**坐标系**。

讨论 1）如果ρ为同构，则其逆映射 ρ^{-1} 也是线性变换，因此也是同构。

2）如果 $\rho: V \to W$ 是同构，令 $\{v_i\}$ 是V的一组基，则不难看出$\{\rho(v_i)\}$是W的一组基。因此我们恒有

$$\dim V = \dim W.$$

反之，容易看出，如果V和W都是K向量空间，且$\dim V = \dim W$，则V和W之间存在一个同构。

3）如果 $\dim V = \infty$，我们可以用别的向量空间当成代数模型，得出V的表示法或坐标系。

定理4.7　1）设 $\dim V = n < \infty$，$\{v_i\}$是V的一组基。则如下的ρ_v：$V \to K^n$是V的一种表示法(坐标系)：

$$\rho_v\left(\sum_i a_i v_i\right) = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} \in K^n.$$

2）设 $\dim W = m < \infty$，$\dim V = n < \infty$。定义 ρ_v：$V \to K^n$ 如上。设$\{w_j\}$是W的一组基，同法定义ρ_w：$W \to K^m$ 如下：

$$\rho_w\left(\sum_i b_j w_j\right) = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix} \in K^m.$$

则 ρ_v, ρ_w 自然引生 $\mathrm{Hom}_K(V, W)$的一种表示法 ρ_{vw} 如下：

$$\rho_{vw}:\ \mathrm{Hom}_K(V, W) \to \mathrm{Hom}_K(K^n, K^m) = \mathrm{FL}(m, n, K).$$

$$\rho_{vw}(\Delta_j^i) = \begin{bmatrix} 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{bmatrix}_{m \times n} \begin{matrix} \\ \\ \\ i \\ \\ \\ \\ \end{matrix} \quad \in \mathrm{Hom}_K(K^n, K^m),$$

（其中 1 位于第 j 列、第 i 行。）

$$\rho_{vw}\left(\sum c_{ij} \Delta_j^i\right) = \sum c_{ij} \rho_{vw}(\Delta_j^i)$$

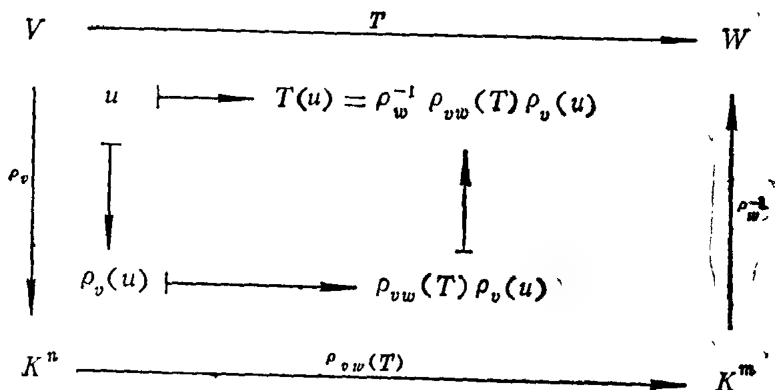
$$= \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{bmatrix} \in \mathrm{Hom}_K(K^n, K^m).$$

上面的m行n列的矩阵中，除了第j行第i列的元素为1以外，其余的元素皆为零。在这里，我们已把$\mathrm{Hom}(K^n, K^m)$认同为$m\times n$阶矩阵的集合$\mathrm{FL}(m, n, K)$。

3）以上我们定义的ρ_{vw}适合下列的关系式：对任意的$T\in \mathrm{Hom}_K(V, W)$，有

$$T(u)=\rho_w^{-1}\rho_{vw}(T)\rho_v(u),\quad \forall u\in V.$$

也即是使下列图形是“交换的”——顺着不同的箭头所指的路线，依次使映射作用，则恒得同一结果：



4）当$V=W$时，令$\mathrm{FL}(n,K)=\mathrm{FL}(n,n,K)$。以上定义的$\rho_{vv}$也保持乘法，即

$$\rho_{vv}(T_1\circ T_2)=\rho_{vv}(T_1)\rho_{vv}(T_2).$$

上式右侧的乘法是一般矩阵的乘法，于是

$$\rho_{vv}:\ \mathrm{Hom}_K(V,V)\to \mathrm{FL}(n,K)$$

是两环的一个同构。

证明 读者自证之。❙

在代数学中，两个同构的数学实体常被认为是相同的。在这种意义下，研究有限维的K向量空间V, W，以及由V到W的线性变换集$\mathrm{Hom}_K(V, W)$，就是研究K^n, K^m及$\mathrm{FL}(m, n, K)$。很

显然，一个线性变换T的矩阵表示式$\rho_{vw}(T)$是随V的基$\{v_i\}$及W的基$\{w_j\}$的选取而变化的。同一线性变换T的不同的矩阵表示式之间，适合下面的定理。

定理4.8 任取V的两组基$\{v_i\}$，$\{v'_i\}$，W的两组基$\{w_j\}$，$\{w'_j\}$。令$T\in \mathrm{Hom}_K(V,W)$，则有下列关系式（参考定理4.7）：

$$T=\rho_w^{-1}\rho_{vw}(T)\rho_v=\rho_{w'}^{-1}\rho_{v'w'}(T)\rho_{v'},$$

即
$$\rho_{vw}(T)=(\rho_w\rho_{w'}^{-1})\rho_{v'w'}(T)(\rho_{v'}\rho_v^{-1}).$$

此处$\rho_w\rho_{w'}^{-1}:K^m\to K^m$，$\rho_{v'}\rho_v^{-1}:K^n\to K^n$是两个自同构。反之，设$A$：$K^m\to K^m$，$B$：$K^n\to K^n$是两个自同构，则$V$有一组基$\{v_i^*\}$，$W$有一组基$\{w_j^*\}$，使

$$\rho_w\rho_{w^*}^{-1}=A,\quad \rho_{v^*}\rho_v^{-1}=B^{-1},$$
$$\rho_{vw}(T)=A(\rho_{v^*w^*}(T))B^{-1}.$$

证明 我们仅证明其后半部。前半部是自明的。如果我们能证明存在一组基$\{w_j^*\}$，使$\rho_w\rho_{w^*}^{-1}=A$。则同法可证存在一组基$\{v_i^*\}$，使$\rho_v\rho_{v^*}^{-1}=B$。于是有

$$\rho_{v^*}\rho_v^{-1}=B^{-1},$$
$$\rho_{vw}(T)=A(\rho_{v^*w^*}(T))B^{-1}.$$

如此，则本定理得证。

因为A是K^m的自同构，所以其逆线性变换A^{-1}是存在的。分别写出A及A^{-1}如下：

$$A=\begin{bmatrix} a_{11} & \cdots & a_{1m}\\ \cdots & \cdots & \cdots\\ a_{m1} & \cdots & a_{mm}\end{bmatrix},\qquad A^{-1}=\begin{bmatrix} c_{11} & \cdots & c_{1m}\\ \cdots & \cdots & \cdots\\ c_{m1} & \cdots & c_{mm}\end{bmatrix}.$$

则有

$$AA^{-1}=A^{-1}A=\begin{bmatrix} 1 & 0 & \cdots & 0\\ 0 & 1 & \cdots & 0\\ \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & \cdots & 1\end{bmatrix}=I.$$

于是令

$$w_j^* = \sum_s a_{sj} w_s, \quad j = 1, 2, \cdots, m,$$

或写为:

$$\begin{bmatrix} w_1^* \\ w_2^* \\ \vdots \\ w_m^* \end{bmatrix} = \begin{bmatrix} \sum a_{s1} w_s \\ \sum a_{s2} w_s \\ \vdots \\ \sum a_{sm} w_s \end{bmatrix} = A^T \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{bmatrix},$$

其中
$$A^T = \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \cdots & \cdots & \cdots & \cdots \\ a_{1m} & a_{2m} & \cdots & a_{mm} \end{bmatrix}.$$

即 A^T 是 A 的转置. 于是有

$$\begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{bmatrix} = (A^{-1})^T \begin{bmatrix} w_1^* \\ w_2^* \\ \vdots \\ w_m^* \end{bmatrix} = \begin{bmatrix} \sum c_{s1} w_s \\ \sum c_{s2} w_s \\ \vdots \\ \sum c_{sm} w_s \end{bmatrix}.$$

(请注意 $(A^T)^{-1} = (A^{-1})^T$.) 显然可证 $\{w_j^*\}$ 是 W 的一组基. 于是 $\rho_w \rho_{w^*}^{-1}: K^m \to K^m$ 是 K^m 的一个自同构. 我们要证明这个自同构与 A 是相等的. 首先我们用这两个自同构作用在 K^m 的标准基上, 即

$$A \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ \vdots \\ a_{mi} \end{pmatrix},$$

$$\rho_w \rho_{w^*}^{-1}\begin{bmatrix}0\\ \vdots\\ 0\\ 1\\ 0\\ \vdots\\ 0\end{bmatrix} = \rho_w(w_i^*) = \rho_w(\sum a_{si} w_s) = \begin{bmatrix}a_{1i}\\ a_{2i}\\ \vdots\\ \vdots\\ a_{mi}\end{bmatrix}.$$

式中A和$\rho_w \rho_{w^*}^{-1}$所作用的向量都是第i个分量为1其它分量均为0的标准基向量。于是有

$$A\begin{bmatrix}0\\ \vdots\\ 0\\ 1\\ 0\\ \vdots\\ 0\end{bmatrix} = \rho_w \rho_{w^*}^{-1}\begin{bmatrix}0\\ \vdots\\ 0\\ 1\\ 0\\ \vdots\\ 0\end{bmatrix}.$$

因此

$$A\begin{bmatrix}f_1\\ f_2\\ \vdots\\ \vdots\\ f_m\end{bmatrix} = f_1 A\begin{bmatrix}1\\ 0\\ \vdots\\ \vdots\\ 0\end{bmatrix} + f_2 A\begin{bmatrix}0\\ 1\\ 0\\ \vdots\\ 0\end{bmatrix} + \cdots f_n A\begin{bmatrix}0\\ 0\\ \vdots\\ 0\\ 1\end{bmatrix}$$

$$= \rho_w \rho_{w^*}^{-1}\begin{bmatrix}f_1\\ f_2\\ \vdots\\ \vdots\\ f_m\end{bmatrix}.$$

于是本定理得证。 ▍

系 设$V=W$，取$\{v_i\}=\{w_j\}$，$\{v'_i\}=\{w'_i\}$。则一线性变换$T\in \mathrm{Hom}_K(V,V)$的两个矩阵表示式$\rho_{vv}(T)$及$\rho_{v'v'}(T)$之间适合下式：

$$\rho_{vv}(T)=A\rho_{v'v'}(T)A^{-1}.$$

此处A是K^n的一个自同构。反之，如已有矩阵M，使

$$\rho_{vv}(T)=AMA^{-1},$$

则有基$\{v'_i\}$，使

$$M=\rho_{v'v'}(T).$$

证明 易于自上定理导出。▎

上面这个系的含意是：域K上的两个矩阵是同一线性变换$T\in \mathrm{Hom}_K(V,V)$的不同的矩阵表示式的充要条件是：这两个矩阵是"相似的"。

定义4.7 设$M,N\in \mathrm{FL}(n,K)$为两个$n\times n$矩阵，如果有一个K^n的自同构$A\in \mathrm{FL}(n,K)$，使下式成立，则称M和N为**相似的**：

$$N=AMA^{-1}.$$

不难看出，矩阵间的相似关系是一个等价关系。一个等价子集表示一个线性变换T。同一个等价子集中的矩阵，从表面上看，是繁简不同的。于是，产生了如何从一个等价子集中，选取简明的、显现线性变换特性的矩阵，以及如何判别两个矩阵是否属于同一等价子集的问题。这就是矩阵的"标准式"的问题。在下面几节，我们将处理这个问题。

例 8 取一常系数的常微分方程式如下：

$$\frac{\mathrm{d}^2 f_1}{\mathrm{d}x^2}-a\frac{\mathrm{d}f_1}{\mathrm{d}x}=bf_1. \tag{1}$$

令

$$\frac{\mathrm{d}f_1}{\mathrm{d}x}=f_2,$$

则(1)可改写成下面的一阶常微分方程组

(2)
$$\begin{cases} \dfrac{df_1}{dx} = f_2, \\ \dfrac{df_2}{dx} = a\dfrac{df_1}{dx} + bf_1 = af_2 + bf_1. \end{cases}$$

或写成向量方程式

(3)
$$\frac{d}{dx}\begin{bmatrix} f_1 \\ f_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ b & a \end{bmatrix}\begin{bmatrix} f_1 \\ f_2 \end{bmatrix} = C\begin{bmatrix} f_1 \\ f_2 \end{bmatrix}.$$

类似地，n阶的常微分方程式

(1′)
$$\frac{d^n f_1}{dx^n} - a_{n-1}\frac{d^{n-1} f_1}{dx^{n-1}} - \cdots - a_i\frac{d^i f_1}{dx^i} - \cdots - a_1\frac{df_1}{dx} = bf_1$$

也可以改写成下列的(3′)：

(3′)
$$\frac{d}{dx}\begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ \vdots \\ f_n \end{bmatrix} = \begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \\ b & a_1 & \cdots & a_{n-1} \end{bmatrix} = C'\begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ \vdots \\ f_n \end{bmatrix}.$$

如有
$$C' = AC''A^{-1},$$
令

$$A^{-1}\begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{bmatrix} = \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_n \end{bmatrix}, \quad \begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{bmatrix} = A\begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_n \end{bmatrix}.$$

则任意的一阶常微分方程组(此处的矩阵C'不限于形如(3′)中的C')：

$$\frac{d}{dx}\begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{bmatrix} = C'\begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{bmatrix},$$

将其两侧乘以 A^{-1} 后，都可化成

$$\frac{\mathrm{d}}{\mathrm{d}x}\begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_n \end{bmatrix} = C''\begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_n \end{bmatrix}.$$

适当选取 C'' 后，此一阶常微分方程组有时很容易解出。我们试举一例：

$$\frac{\mathrm{d}}{\mathrm{d}x}\begin{bmatrix} f_1 \\ f_2 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} f_1 \\ f_2 \end{bmatrix} = C'\begin{bmatrix} f_1 \\ f_2 \end{bmatrix}.$$

从线性代数我们知道下式

$$\begin{aligned} C' &= \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \\ &= \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}\begin{bmatrix} 3 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \\ &= AC''A^{-1}. \end{aligned}$$

令

$$A^{-1}\begin{bmatrix} f_1 \\ f_2 \end{bmatrix} = \begin{bmatrix} g_1 \\ g_2 \end{bmatrix}, \quad \begin{bmatrix} f_1 \\ f_2 \end{bmatrix} = A\begin{bmatrix} g_2 \\ g_2 \end{bmatrix}.$$

则 g_1, g_2 满足的方程式为

$$\frac{\mathrm{d}}{\mathrm{d}x}\begin{bmatrix} g_1 \\ g_2 \end{bmatrix} = \begin{bmatrix} 3 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} g_1 \\ g_2 \end{bmatrix} = \begin{bmatrix} 3g_1 \\ -g_2 \end{bmatrix}.$$

即

$$\frac{\mathrm{d}g_1}{\mathrm{d}x} = 3g_1, \quad \frac{\mathrm{d}g_2}{\mathrm{d}x} = -g_2.$$

此方程式易解，得

$$g_1 = k_1 e^{3x}, \quad g_2 = k_2 e^{-x}.$$

于是

$$f_1 = \frac{1}{\sqrt{2}} k_1 e^{3x} - \frac{1}{\sqrt{2}} k_2 e^{-x}, \quad f_2 = \frac{1}{\sqrt{2}} k_1 e^{3x} + \frac{1}{\sqrt{2}} k_2 e^{-x}.$$

习　题

1. 设$\varepsilon_1,\varepsilon_2,\varepsilon_3,\xi_1,\xi_2,\xi_3$如§2习题9。设有线性变换$T$，使得

$$T(\varepsilon_1) = \varepsilon_1 + 2\varepsilon_2 - 3\varepsilon_3,$$
$$T(\varepsilon_2) = 2\varepsilon_1 - 3\varepsilon_2 + \varepsilon_3,$$
$$T(\varepsilon_3) = \varepsilon_1 + \varepsilon_2.$$

写出变换矩阵$\rho_{\varepsilon\varepsilon}(T)$及$\rho_{\xi\xi}(T)$。验证$\rho_{\varepsilon\varepsilon}(T) = A\rho_{\xi\xi}(T)A^{-1}$，其中$A$为由基$\{\varepsilon_1,\varepsilon_2,\varepsilon_3\}$到基$(\xi_1,\xi_2,\xi_3)$的**过渡矩阵**，即$A$满足

$$(\xi_1,\xi_2,\xi_3) = (\varepsilon_1,\varepsilon_2,\varepsilon_3)A.$$

2. 设A为二阶复方阵。在$\mathrm{FL}(2,\boldsymbol{C})$中定义变换$T$如下：

$$T(X) = AX - XA, \quad X \in \mathrm{FL}(2,\boldsymbol{C}).$$

(1) 试证明T是线性变换；

(2) 取$\mathrm{FL}(2,\boldsymbol{C})$的一组基如下：

$$\boldsymbol{\varepsilon}_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \boldsymbol{\varepsilon}_2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},$$

$$\boldsymbol{\varepsilon}_3 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad \boldsymbol{\varepsilon}_4 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

试写出T在这组基下的矩阵$\rho_{\varepsilon\varepsilon}(T)$。

3. 设A,B是两个$n\times n$矩阵，适合$A(AB-BA)=(AB-BA)A$。证明对任何正整数n而言，恒有

$$A^nB - BA^n = nA^{n-1}(AB-BA).$$

4. 设A是$n\times n$矩阵，I为$n\times n$阶幺矩阵。证明，如果

$$A^2(I-A)=A(I-A)^2,$$

则 A 必是幂幺的(idempotent)，即存在正整数 n，使得 $A^n=I$。

5. 令

$$\mathcal{C}=\{A:\ A\in \mathrm{FL}(2,\boldsymbol{C}),\ AB=BA,\ \forall B\in \mathrm{FL}(2,\boldsymbol{C})\}.$$

称 $\mathcal{C}$ 为环 $\mathrm{FL}(2,\boldsymbol{C})$ 的**中心**(center)。证明

$$\mathcal{C}=\{\lambda I:\ \lambda\in \boldsymbol{C}\},$$

其中 I 为 2×2 阶幺矩阵。

6. 设 A,B,C,D 是向量空间 V 的线性变换。如果 $A+B$ 和 $A-B$ 都是可逆的，证明存在线性变换 X,Y，使得

$$AX+BY=C,\quad BX+AY=D.$$

7. 设 A 是向量空间 K^n 的线性变换。我们称 $\dim(\mathrm{im}(A))$ 为 A 的**秩**，记为 $r(A)$。设又有线性变换 B，使得 $AB=0$，证明

$$r(A)+r(B)\leqslant n.$$

8. 设 A 为 $n\times n$ 矩阵。如果 $A^2=A$，则称 A 是一个**投影**(projection)。令

$$\sigma:\ \boldsymbol{R}^n\to\boldsymbol{R}^n,$$

$$(a_1,\cdots,a_n)\mapsto(a_1,\cdots,a_m,0,\cdots,0).$$

证明 σ 的矩阵是一个投影。

9. 参考上题：设 A 是一个投影，证明 $I-A$ 也是一个投影，这里 I 是幺矩阵。

10. 设线性变换 A 是向量空间 K^n 的一个投影，证明

$$K^n=\mathrm{im}(A)\oplus\mathrm{im}(I-A).$$

11. 设 f 是向量空间 V 的一个线性函数。定义线性变换

$$A(v)=f(v)v_0,$$

其中 v_0 是 V 中一个确定的向量。试问如果 A 是一个投影，f 及 v_0 必须适合什么条件？

12. 下面的两个矩阵是相似的吗？

$$\begin{bmatrix} 1 & 0 & 2 & 0 & 3 \\ 0 & 0 & 4 & 5 & 0 \\ -1 & 1 & 1 & 0 & 0 \\ 2 & 3 & 4 & 0 & 5 \\ 3 & 4 & 3 & 2 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

13．若A是可逆矩阵，证明AB与BA相似。

14．若A与B相似，C与D相似，证明分块矩阵

$$\begin{bmatrix} A & 0 \\ 0 & C \end{bmatrix} \text{与} \begin{bmatrix} B & 0 \\ 0 & D \end{bmatrix}$$

相似。

15．设A矩阵与B相似，$f(x)$是一元多项式，证明$f(A)$与$f(B)$相似。

16．找出两个矩阵A，B，使得A^2与B^2相似，但A与B不相似。

§4 模及主理想环上的模

一些数学与科学上的问题，如果局限在小范围内，常常越弄越繁，不容易理出头绪来．另一方面，如能打破框框，走入更广阔，因此也更抽象的道路，则有时候立见真章了。对于矩阵的"标准式"的问题，我们采取扩大范围考虑问题的方法，引入如下的定义。

定义4.8 设R是一交换环．一个非空的集合M，如适合下列条件，则称为R**模**，或简称为**模**：

1）M中有加法"+"。而对"+"而言，M是一交换群．令其幺元为0；

2）任取$a\in R$，$m\in M$，有一双项运算（通常称为乘法"·"）存在，使$a\cdot m\in M$，及$1\cdot m=m$，此处1是R的乘法的幺元（乘

法符号“·”经常忽略不写)；

3）这四种运算：交换环R的加法、乘法，M的加法及R与M之间的乘法都适合结合律及分配律，即

$$(a_1a_2)m = a_1(a_2m), \quad (a_1 + a_2)m = a_1m + a_2m,$$
$$a(m_1 + m_2) = am_1 + am_2.$$

讨论 比较定义4.8及定义4.1，模与向量空间是很类似的。其主要差别是模M只要求一个交换环R作常量，而向量空间V是有一个常数域作常量。例如，向量空间的最重要的概念“维数”，就不能完全地推广到模上。参见下定义。

定义4.9 设$S = \{m_i: i \in I\}$是模M的子集。如果M的任意元素m皆可写成

$$m = \sum_{\text{有限}} a_i m_i, \quad a_i \in R, \quad m_i \in S,$$

则称S是M的**生成元集**。如果M有一有限的生成元集，则称M是**有限生成的模**.

讨论 $\boldsymbol{R}[x]$是一个$\boldsymbol{R}[x]$模。此模可以由$\{1\}$生成，也可以由$\{x, 1-x\}$生成，即

$$f(x) = f(x) \cdot 1;$$
$$f(x) = f(x) \cdot x + f(x)(1-x).$$

不仅$\{1\}$是$\boldsymbol{R}[x]$的一个极小生成元集，而且$\{x, 1-x\}$也是，即从$\{x, 1-x\}$中去掉x或$1-x$，则其“余集”不成为生成元集。如此，这两个极小的生成元集有不同的基数，与向量空间的情形很不一样。因此，模的“维数”的概念，不能像向量空间的维数概念一样地界定了。

例9 设R为一交换环，I是R的理想。则I自然是一个R模。于是，关于R模的任何定理皆适用理想I。反之，任何已知的关于理想I的定理，也应该验证能不能推广到模M上。

设I是R的理想，定义R在商环R/I上的作用

$$a\rho(r)=\rho(ar),$$

这里 ρ 是自 R 到 R/I 的典型映射，$a,r\in R$。R/I 因此成为 R 模。

设 $M_1,\cdots,M_n$ 皆是 R 模，则 $M_1\times\cdots\times M_n$ 也是 R 模，其运算定义如下：

$$(m_1,\cdots,m_n)+(m'_1,\cdots,m'_n)=(m_1+m'_1,\cdots,m_n+m'_n),$$

$$a(m_1,\cdots,m_n)=(am_1,\cdots,am_n).$$

例10 设 G 是交换群。则 G 自然成为 $\boldsymbol{Z}$ 模如下：

$$ng=g+g+\cdots+g,\qquad -ng=(-g)+(-g)+\cdots+(-g),$$

$$n\in\boldsymbol{Z},\quad n\geqslant 0,\quad g\in G.$$

上二式右侧的项数皆为 n。

例11 设 $A\in\mathrm{Hom}(K^n,K^n)=\mathrm{FL}(n,K)$ 为作用在 K 向量空间 K^n 上的线性变换。则通过 A 的如下作用，K^n 成为一 $K[x]$ 模：

$$f(x)v=f(A)v,\quad \forall f(x)\in K[x],\ v\in K^n.$$

上式是 $f(x)v$ 的定义，其右侧自然是

$$f(A)v=\left(\sum_i a_iA^i\right)v=\sum_i a_i(A^iv),$$

此时

$$f(x)=\sum_i a_ix^i.$$

对于不同的 A，用上法建构的模 V，就集合而言，是同一集合 K^n，其环也是同一环 $K[x]$。但是，环 $K[x]$ 与集合 K^n 之间的乘法是因 A 而异的。所以如此建构的模也根本不同了。我们正是要从这些模的差异处，导出 A 的"初等因子"、"挠因子"及"若当标准式"。其详情请见下一节。现在我们要举例以更具体地显示这些模的差异性。以下设 $n=2$。

1）设

$$A=I=\begin{bmatrix}1&0\\0&1\end{bmatrix},$$

则有

$$f(x)v=\left(\sum_i a_ix^i\right)v=\left(\sum_i a_iI^i\right)v=\left(\sum_i a_i\right)v.$$

即其乘法的结果，仅是乘以常数$\sum a_i$。不难看出，此模的生成元集的基数最少是2。

2）设
$$A=J=\begin{bmatrix}0&1\\1&0\end{bmatrix},$$
则有
$$x\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}0&1\\1&0\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}0\\1\end{bmatrix},$$
$$x\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}0&1\\1&0\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}1\\0\end{bmatrix}.$$
不难看出，此模可以由
$$\left\{\begin{bmatrix}1\\0\end{bmatrix}\right\}$$
生成，即
$$\begin{bmatrix}a_1\\a_2\end{bmatrix}=(a_1+a_2x)\begin{bmatrix}1\\0\end{bmatrix}. \quad \blacksquare$$

一般的模的理论是很有意义的。我们为了解决线性代数的问题，主要考虑环R是主理想环时模的理论。因为$\boldsymbol{Z}$及$K[x]$皆是主理想环，所以，以下关于主理想环的模的定理皆适用例10及例11中所举的交换群及向量空间。然而，为了清晰明白地叙述数学证明，我们先给出一般的模的理论所用的术语及概念，然后再研究R是主理想环的特殊情形。

定义4.10 设M是R模。如果M的一个非空的子集N对同样的加法及乘法也成为模，则称N为M的**子模**。

定义4.11 设$\rho: M\to M'$是自R模M到R模M'的映射。如果ρ对于交换群M, M'而言是群映射，并且保持其乘法的关

系，即

$$\rho(am)=a\rho(m),\quad \forall a\in R,\ m\in M,$$

则称 ρ 为**模映射**。设 ρ 为模映射。若 ρ 为单射，则称 ρ 为**模单射**；若 ρ 为满射，则称 ρ 为**模满射**；若 ρ 为单满映射，则称 ρ 为**模同构**，此时称 M 与 M' **同构**。

设 ρ: $M\to M'$ 是模映射，则 ρ 的**核** $\ker(\rho)$ 定义为

$$\ker(\rho)=\{m:\ m\in M,\ \rho(m)=0\in M'\}.$$

ρ 的**象** $\mathrm{im}(\rho)$ 定义为

$$\mathrm{im}(\rho)=\{m':\ m'\in M',\ \text{存在 } m\in M,\ \text{使 } \rho(m)=m'\}.$$

以上几个概念，已在群论、环论、向量空间论中反复出现。这些是代数的基本概念。以下我们也要如常地导出"商模"及"同构定理"等等。

设 N 是 M 的子模。单就加法群的结构来研究，商群 M/N 自然是存在的。很容易看出 M/N 也自然地是 R 模。我们定义乘法如下：

$$a[m]=[am],\quad \forall a\in R,\ [m]\in M/N.$$

我们先验证这个定义是良好的。设 $[m_1]=[m_2]$，则

$$m_1-m_2\in N.$$

乘以 a，得

$$am_1-am_2\in aN\subset N \iff [am_1]=[am_2].$$

所以这个定义是良好的。很容易验证模的定义（定义4.8）的其余条件。于是我们有

定义4.12 设 N 是 M 的子模。则 M 对于 N 的**商模** M/N 定义为：M/N 的群即商群 M/N，乘法为

$$a[m]=[am].$$

定理4.9 设 ρ: $M\to M'$ 为模映射。$\bar\rho$: $M/\ker(\rho)\to \mathrm{im}(\rho)$ 定义为

$$\bar\rho([m])=\rho(m).$$

则 $\bar\rho$ 是一单满映射。于是 $M/\ker(\rho)$ 与 $\mathrm{im}(\rho)$ 同构。如果 M 及 M'

皆是K向量空间，ρ是线性变换，则恒有

$$\dim M = \dim \ker(\rho) + \dim \operatorname{im}(\rho).$$

证明 我们仅证明此定理的后半部。任取$\ker(\rho)$的一组基$\{v_1,\cdots,v_m,\cdots\}$（如$\ker(\rho)=\{0\}$时，其基为空集），把它扩充成$M$的基$\{v_1,\cdots,v_m,\cdots\}\cup\{u_1,\cdots,u_n,\cdots\}$。我们要证明$\{\rho(u_1),\cdots,\rho(u_n),\cdots\}$是$\operatorname{im}(\rho)$的一组基。如此则有

$$\begin{aligned}\dim M &= \{v_1,\cdots,v_m,\cdots\}\text{的基数}+\{u_1,\cdots,u_n,\cdots\}\text{的基数}\\ &= \dim \ker(\rho)+\dim \operatorname{im}(\rho).\end{aligned}$$

显然的，$\{\rho(u_1),\cdots,\rho(u_m),\cdots\}$是$\operatorname{im}(\rho)$的生成元集，所以我们仅须证明它是线性无关集。事实上

$$\sum_i a_i\rho(u_i)=0 \Longrightarrow \rho\left(\sum_i a_iu_i\right)=0 \Longrightarrow \sum_i a_iu_i\in\ker(\rho)$$

$$\Longrightarrow \sum_i a_iu_i=\sum_j b_jv_j.$$

而$\{v_1,\cdots,v_m,\cdots\}\cup\{u_1,\cdots,u_n,\cdots\}$是$M$的基，所以是线性无关集，故有

$$a_i=0,\quad b_j=0,\quad \forall i,j.$$

所以$\{\rho(u_1),\cdots,\rho(u_n),\cdots\}$是线性无关集。▎

如果M有子模M_1及M_2，使由典型映射ρ: $M\to M/M_1$引生的映射ρ: $M_2\to M/M_1$为同构，则自然有

1) $M_1\cap M_2=\{0\}$；

2) $M_1\cup M_2$生成M。

反之，如果M_1,M_2适合条件1)与2)，则ρ: $M_2\to M/M_1$是同构。请注意，1),2)对于M_1,M_2是对称的，所以我们也有M_1与M/M_2同构。在此情形下，我们称M是M_1与M_2的**直积**，它与$M_1\times M_2$同构。

一种重要而且简单的模是“自由模”。我们仅研究有限生成的自由模，定义如下。

定义4.13 任何与$R^n=R\times R\times\cdots\times R$同构的$R$模$M$，称为(**有限生成的)自由$R$模**。令$e_1=(1,0,\cdots,0),\cdots,e_i=(0,\cdots,0,1,0,\cdots,0),\cdots,e_n=(0,\cdots,0,1)\in R^n$，$\rho$: $R^n\to M$为同构映射。则称$\{\rho(e_1),\cdots,\rho(e_i),\cdots,\rho(e_n)\}$为$M$的一组**基**。

给定一个R模M，则其不同的极小的生成元集不一定有相同的基数。在自由模的特殊情况下，基的基数是相同的。我们有如下的定理。

定理4.10 设M是自由R模，令ρ: $R^n\to M$及ρ': $R^{n'}\to M$是两个同构映射，则$n=n'$，即自由模的基的基数是相同的。

证明 在R中任取一极大理想I(参考定理3.23)。令其商域R/I为K(参考定理3.24)。又令

$$N=I\cdot M=\left\{\sum_{\text{有限}}i_jm_j:\ i_j\in I,\ \ m_j\in M\right\}.$$

不难看出N是M的子模，于是商模$L=M/N$也是R模。不仅如此，L也可以自然地成为一个K向量空间：令R中的元素为a, b, c, $\cdots$，K中的元素为$[a],[b],[c],\cdots$，M中的元素为$m_1,m_2,\cdots$，L中的元素为$[m_1],[m_2],\cdots$。则可定义

$$[a][m_1]=[am_1],\quad \forall\ [a]\in K,\ [m_1]\in L.$$

当然，我们应该验证这个定义是良好的。这是不难的，令

$$[b]=[a],\quad [m_1]=[m_2],$$

则

$$b-a\in I,\quad m_1-m_2\in N.$$

于是

$$am_1-bm_2=a(m_1-m_2)+(a-b)m_2\in N+I\cdot M=N.$$

所以这是一个良好的定义。同理$R^n/I\cdot R^n$也是K向量空间，事实上就是K^n。考虑ρ及ρ'两个同构，它们引生了以下两个向量空间的同构：

$$K^n\approx L,\qquad K^{n'}\approx L.$$

于是$n=n'$。▎

定理4.11 设 M 是 R 模，$m_1,m_2,\cdots,n_n\in M$。则 M 是自由模以及 $\{m_1,m_2,\cdots,m_n\}$ 是 M 的基的充要条件是：$\{m_1,m_2,\cdots,m_n\}$ 是 M 的生成元集，以及如果有下列等式时：

$$a_1m_1+a_2m_2+\cdots+a_nm_n=0,\quad a_i\in R,$$

则必有 $a_1=a_2=\cdots=a_n=0$。

证明 如果有 ρ: $R^n\to M$ 为同构映射，使

$$\rho(e_1)=m_1,\quad \rho(e_2)=m_2,\quad \cdots,\quad \rho(e_n)=m_n,$$

此处

$$e_1=(1,0,\cdots,0),\ e_2=(0,1,0,\cdots,0),\cdots,\ e_n=(0,\cdots,0,1),$$

则有

$$\rho\left(\sum_i b_ie_i\right)=\sum_i b_im_i,\quad b_i\in R.$$

而 ρ 为满射，故 $\{m_1,m_2,\cdots,m_n\}$ 自然是生成元集。又，如果

$$\sum_i a_im_i=0,$$

则有

$$\rho\left(\sum_i a_ie_i\right)=\sum_i a_im_i=0.$$

而 ρ 是单射，所以必有

$$(a_1,a_2,\cdots,a_n)=\sum_i a_ie_i=0,$$

即 $a_1=a_2=\cdots=a_n=0$。

反之，如果 $\{m_1,m_2,\cdots,m_n\}$ 适合本定理的两个条件，令 ρ^*: $R^n\to M$ 定义为

$$\rho^*((b_1,b_2,\cdots,b_n))=\rho^*\left(\sum_i b_ie_i\right)=\sum_i b_im_i.$$

则易于看出 ρ^* 是一个模映射。因为 $\{m_1,m_2,\cdots,m_n\}$ 是生成元集，所以 ρ^* 是满射。现在我们要证明 $\ker(\rho)=\{0\}$，如此，则 ρ^* 是一个单射。令 $(a_1,a_2,\cdots,a_n)\in\ker(\rho^*)$，则有

$$0=\rho^*(a_1,a_2,\cdots,a_n)=\sum_i a_i m_i.$$

于是 $a_1=a_2=\cdots=a_n=0$，即 $\ker(\rho)=\{0\}$。 ▎

任取一有限生成的 R 模 M。设 $\{m_1,m_2,\cdots,m_n\}$ 为一生成元集，则可定义

$$\rho:\ R^n\to M,$$

$$\rho(e_i)=m_i,\quad i=1,2,\cdots,n,$$

此处 $e_1=(1,0,\cdots,0)$，$e_2=(0,1,0,\cdots,0),\cdots$，$e_n=(0,\cdots,0,1)$。按照定理4.9，我们恒有

$$R^n/\ker(\rho)\approx M.$$

于是研究模 M，不外乎研究一个自由模 R^n 的商模，其实也就是研究一个自由模 R^n 的子模 $\ker(\rho)$的某些性质。在环 R 是主理想整环时，我们有如下的定理。

定理4.12 设 R 是一个主理想整环，M 是一个有限生成的自由 R 模，N 是 M 的一个非零的子模，则存在 M 的一组基 $\{m_1,m_2,\cdots,m_n\}$ 及 $c_1,c_2,\cdots,c_l\in R(l\leqslant n)$，使

1) $c_1|c_2|\cdots|c_l$；

2) N 是由 $c_1m_1,c_2m_2,\cdots,c_lm_l$ 生成的模。

证明 如果 $n=1$，设 $M=R\cdot m_1$。令

$$I=\{c:\ c\in R,\ cm_1\in N\}.$$

易验证 I 是 R 的一个理想。设 $I=(c_1)$，则 N 是由 c_1m_1 生成的。于是令 $l=1$，即得本定理。

我们对 n 作数学归纳法。设 $n>1$。任取 M 的一组基

$$\{\tilde{m}_1,\tilde{m}_2,\cdots,\tilde{m}_n\},$$

再任取其中一个元素 $\tilde{m}_i$。令

$$J=\Big\{c_i\in R:\ \text{存在 } m\in N \text{ 及 } c_1,\cdots,c_{i-1},c_{i+1},\cdots,c_n\in R,$$

$$使\ m=\sum_{j=1}^{n}c_j\bar{m}_j\Big\},$$

这相当于向量空间向某一固定的 i 轴的投影。对 M 的所有可能的基和所有的 i 得到的所有 J 的集合记为 $\mathscr{I}$。易于看出 $\mathscr{I}$ 中的元素都是 R 的理想。因为 R 是主理想环，所以是诺德环（定义3.21），于是在 $\mathscr{I}$ 的所有元素中，有一极大者（定理3.25）。令此极大者为 I^*，则 I^* 显然不是(0)。所以，若令

$$I^*=(c_1),$$

则 $c_1\neq 0$。设 I^* 所对应的 M 的基为 $\{m_1^*,m_2^*,\cdots,m_n^*\}$，适当地排列这些基元素的顺序，无妨设 I^* 是 N 的元素表为这组基的线性组合时 m_1^* 的系数的集合。于是有一 $m\in N$，使

(1) $$m=c_1m_1^*+c_2^*m_2^*+\cdots+c_n^*m_n^*.$$

我们来证明，在上式中恒有

(2) $$c_1|c_i^*,\quad i=2,3,\cdots,n.$$

以下我们证明 $c_1|c_2^*$。同法可证其余。令 $(d)=(c_1,c_2^*)$，则有

(3) $$d=\alpha c_1+\beta c_2^*,\quad \alpha,\beta\in R.$$

(4) $$c_1=\delta d,\quad c_2^*=\varepsilon d,\quad \delta,\varepsilon\in R.$$

由(3)及(4)式可得

$$1=\alpha\delta+\beta\varepsilon.$$

令 $m_1,m_2,\cdots,m_n$ 由下式所定:

(5) $$m_1=\delta m_1^*+\varepsilon m_2^*,\ m_2=-\beta m_1^*+\alpha m_2^*,\ m_i=m_i^*,\quad \forall i>2.$$

即

(6) $$m_1^*=\alpha m_1-\varepsilon m_2,\ m_2^*=\beta m_1+\delta m_2,\ m_i^*=m_i,\quad \forall i>2.$$

我们先证明 $\{m_1,m_2,\cdots,m_n\}$ 也是 M 的基，然后再考虑(1)式中的 m 对这组基的展开式。从(6)式立得 $\{m_1,m_2,\cdots,m_n\}$ 是 M 的生成元集。再设有

(7) $$a_1m_1+a_2m_2+\cdots+a_nm_n=0,$$

以(5)式代入，得

$$(a_1\delta - a_2\beta)m_1^* + (a_1\varepsilon + a_2\alpha)m_2^* + a_3m_3^* + \cdots + a_nm_n^* = 0.$$

由于$\{m_1^*, m_2^*, \cdots, m_n^*\}$是基，根据定理4.11，得出

(8) $$a_1\delta - a_2\beta = 0,\ a_1\varepsilon + a_2\alpha = 0,\ a_3 = a_4 = \cdots = a_n = 0.$$

由(8)式中的前两个方程，得

$$a_1 = 0, \quad a_2 = 0.$$

于是得出 $a_1 = a_2 = \cdots = a_n = 0$。根据定理 4.11，即知$\{m_1, m_2, \cdots, m_n\}$是 M 的一组基。现考虑 m 对$\{m_1, m_2, \cdots, m_n\}$的展开式，

$$\begin{aligned} m &= c_1m_1^* + c_2^*m_2^* + \cdots + c_n^*m_n^* \\ &= (\alpha c_1 + \beta c_2^*)m_1 + (-\varepsilon c_1 + \delta c_2^*)m_2 + c_3^*m_3 + \cdots + c_n^*m_n \\ &= dm_1 + (-\varepsilon c_1 + \delta c_2^*)m_2 + c_3^*m_3 + \cdots + c_n^*m_n. \end{aligned}$$

令

$$J' = \{c \in R: 存在\ m' \in N\ 及\ \bar{c}_2, \cdots, \bar{c}_n \in R,\ 使\ m' = cm_1 + \bar{c}_2m_2 + \cdots + \bar{c}_nm_n\},$$

则 $d \in J'$。由(4)式又知 $I^* = (c_1) \subset (d)$，故有

$$I^* \subset (d) \subset J' \in \mathscr{F}.$$

而 I^* 是 $\mathscr{F}$ 中的极大者，所以必有

$$I^* = (c_1) = (d) = J'.$$

于是 c_1 与 d 为相伴元素。由(4)式，立得

$$c_1 | d | c_2^*.$$

令

$$c_i^* = c_1d_i^*, \quad i = 2, 3, \cdots, n, \quad d_i^* \in R.$$

再令

$$\bar{m}_1 = m_1^* + \sum_{i=2}^{n} d_i^*m_i^*, \quad \bar{m}_i = m_i^*, \quad i = 2, 3, \cdots, n.$$

又令 M_1 是$\{\bar{m}_2, \cdots, \bar{m}_n\}$生成的子模，则有

$$m = c_1\bar{m}_1, \quad m_1^* = \bar{m}_1 - \sum_{i=2}^{n} d_i^*\bar{m}_i,$$

$$m_i^* = \bar{m}_i, \quad \forall i \geqslant 2.$$

不难看出$\{\bar{m}_1, \bar{m}_2, \cdots, \bar{m}_n\}$也是 M 的基。令

$$N_1 = M_1 \cap N,$$

则 N_1 自然是 M_1 的子模。

我们现在可以应用数学归纳法了，因为 M_1 是由M的基$\{\bar{m}_1, \bar{m}_2, \cdots, \bar{m}_n\}$的子集$\{\bar{m}_2, \cdots, \bar{m}_n\}$生成的，所以根据定理4.11，$M_1$ 是自由模。如果 N_1 是零模，不难看出，N 是由 $c_1\bar{m}_1$ 生成的子模(请参看本定理(13)式的证明)。取 $l=1$，即得本定理。如果 N_1 不是零模，根据归纳法假设，我们有 M_1 的一组基$\{\hat{m}_2, \cdots, \hat{m}_n\}$及 $c_2, c_3, \cdots, c_l \in R$，使

(9) $$c_2 | c_3 | \cdots | c_l,$$

(10) N_1 是由 $c_2\hat{m}_2, c_3\hat{m}_3, \cdots, c_l\hat{m}_l$ 生成的模。

为了证明本定理，我们仅须证明以下三点：

(11) $\{\bar{m}_1, \hat{m}_2, \hat{m}_3, \cdots, \hat{m}_n\}$是 M 的一组基，

(12) $$c_1 | c_2,$$

(13) N 是由 $c_1\bar{m}_1, c_2\hat{m}_2, \cdots, c_l\hat{m}_l$ 生成的模。

先证(11)。不难看出，$\bar{m}_1, \bar{m}_2, \cdots, \bar{m}_n$皆在由$\{\bar{m}_1, \hat{m}_2, \cdots, \hat{m}_n\}$生成的子模内，而$\{\bar{m}_1, \bar{m}_2, \cdots, \bar{m}_n\}$是 M 的生成元集，故$\{\bar{m}_1, \hat{m}_2, \cdots, \hat{m}_n\}$是$M$的生成元集。又令

$$d_1\bar{m}_1 + d_2\hat{m}_2 + \cdots + d_n\hat{m}_n = 0.$$

由此得

$$-d_1\bar{m}_1 = \sum_{i=2}^{n} d_i \hat{m}_i \in M_1,$$

因而 $$d_1 = 0, \quad d_2 = d_3 = \cdots = d_n = 0.$$

于是，根据定理4.11，(11)得证。再证(12)。取

$$m' = c_1\bar{m}_1 + c_2\hat{m}_2 \in N,$$

用证明(2)式的方法，立得 $c_1 | c_2$。最后，我们来证(13)。任取

$m'' \in N$，把 m'' 表成$\{m_1^*, m_2^*, \cdots, m_n^*\}$的展开式：

$$m'' = f_1 m_1^* + f_2 m_2^* + \cdots + f_n m_n^*.$$

按照 I^* 的定义，$f_1 \in (c_1)$，令 $f_1 = g c_1$。以$\{\bar{m}_1, \cdots, \bar{m}_n\}$取代$\{m_1^*, \cdots, m_n^*\}$后，$m''$ 的展开式是

$$\begin{aligned} m'' &= f_1 \bar{m}_1 + (f_2 - f_1 d_2^*)\bar{m}_2 + \cdots + (f_n - f_1 d_n^*)\bar{m}_n \\ &= g_1(c_1 \bar{m}_1) + (f_2 - f_1 d_2^*)\bar{m}_2 + \cdots + (f_n - f_1 d_n^*)\bar{m}_n. \end{aligned}$$

从此得出 $m'' - g_1(c_1 \bar{m}_1) \in M_1 \cap N = N_1$。于是 $m'' - g_1(c_1 \bar{m}_1)$ 可以写成 $g_2 c_2 \hat{m}_2 + \cdots + g_l c_l \hat{m}_l$，即

$$m'' = g_1(c_1 \bar{m}_1) + g_2(c_2 \hat{m}_2) + \cdots + g_l(c_l \hat{m}_l). \quad \blacksquare$$

定理4.13（主理想整环上有限生成模的基本定理） 设R是一个主理想整环，M是一个有限生成的R模。则存在 $c_1, c_2, \cdots, c_l \in R$，使

1) $c_1 | c_2 | \cdots | c_l$，c_l 皆不可逆；

2) M 与 $R/(c_1) \times R/(c_2) \times \cdots \times R/(c_l) \times R \times \cdots \times R$同构。

证明 设M是由 $\{m_1, \cdots, m_s\}$ 生成的。令 ρ: $R^s \to M$ 为如下定义的模满射：设 $e_1 = (1, 0, \cdots, 0)$，$e_2 = (0, 1, 0, \cdots, 0)$，$\cdots$，$e_s = (0, 0, \cdots, 0, 1) \in R^s$，令

$$\rho(e_i) = m_i, \quad i = 1, 2, \cdots, s.$$

令 ρ 的核 $\mathrm{her}(\rho) = N$，于是有下列的同构：

$$M \approx R^s / N.$$

根据定理4.12，存在 R^s 的基 $\{e_1', e_2', \cdots, e_s'\}$及$c_1, c_2, \cdots, c_{l'} \in R$，使

1′) $c_1 | c_2 | \cdots | c_{l'}$；

2′) N 是 $c_1 e_1', c_2 e_2', \cdots, c_{l'} e_{l'}'$ 生成的模。

定义映射

$$\sigma: R^s \to R/(c_1) \times R/(c_2) \times \cdots \times R/(c_{l'}) \times \overbrace{R \times \cdots \times R}^{(s-l')\text{个}},$$

$$\sigma\left(\sum_i a_i e_i'\right) = ([a_1]_1, [a_2]_2, \cdots, [a_{l'}]_{l'}, a_{l'+1}, \cdots, a_s),$$

此处$[a_i]_i$是a_i在$R \to R/(c_i)$下的象。显然，这是一个模满射，而其核也显然是N，于是有下列的同构：

$$M \approx R^t/N \approx R/(c_1) \times R/(c_2) \times \cdots \times R/(c_{l'}) \times R \times \cdots \times R.$$

在上式中，可能前几个$c_1, \cdots, c_r$皆可逆，于是理想$(c_1) = \cdots = (c_r) = R$，而相应的商模$R/(c_1), \cdots, R/(c_r)$皆是零模。把这些$c_1, \cdots, c_r$及相应的商模弃去后，即得本定理。❙

定理4.14（有限生成的交换群的基本定理） 设G是一个有限生成的交换群，则存在$c_1, c_2, \cdots, c_l \in \boldsymbol{Z}$，使

1) $c_1 | c_2 | \cdots | c_l$，$c_1 > 1$；

2) G与$\boldsymbol{Z}/(c_1) \times \boldsymbol{Z}/(c_2) \times \cdots \times \boldsymbol{Z}/(c_l) \times \boldsymbol{Z} \times \cdots \times \boldsymbol{Z}$同构。

证明 这是定理4.13的特例。❙

定理4.13及定理4.14中提到的$c_1, c_2, \cdots, c_l$被称为模M及群G的**挠因子**。以后我们将要证明这些"挠因子"在条件1)的限制下，是由模M及群G唯一确定的。我们先解释名词"挠因子"的意义。

定义4.14 设R是一交换环，M是R模。任取$S \subset M$，S的消灭子$\mathrm{Ann}(S)$定义为

$$\mathrm{Ann}(S) = \{a:\ a \in R,\ as = 0,\ \forall s \in S\}.$$

如果$m \in M$，而m的消灭子$\mathrm{Ann}(m) \neq \{0\}$，则称$m$为**挠元素**。

讨论 1) 设G是$\boldsymbol{Z}$模（即交换群），则元素g的消灭子$\mathrm{Ann}(g)$与g的阶$o(g)$几乎是一样的，只是消灭子$\mathrm{Ann}(g) = \{0\}$时，相当于$o(g)$为无穷大。

2) 设R为一整环，则R模M中的挠元素的集合是一个子模。这点不难证明：任取挠元素$m_1, m_2 \in M$，取$a_1 \in \mathrm{Ann}(m_1)$，$a_2 \in \mathrm{Ann}(m_2)$，$a_1 \neq 0$，$a_2 \neq 0$，于是有

$$a_1 a_2 (m_1 + m_2) = 0, \quad a_1 (c m_1) = c (a_1 m_1) = 0.$$

所以挠元素的集合是一个子模，称之为M的**挠子模**。于是，交换群的有限阶的元素构成一个**挠子群**。

3) 易于看出，定义4.14中的$\mathrm{Ann}(S)$是R的一个理想。主理

想整环上的有限生成模的挠因子就是其挠子模的某些子集的消灭子（作为理想）的生成元。

4）“代数拓扑学”中应用“同调群”的概念。在良好的拓扑空间上，同调群是有限生成的交换群。定理4.14在这里有很好的应用价值。此时，挠因子称为**挠数**，而定理4.14的条件2)中的 $\boldsymbol{Z}$ 的个数称为**贝蒂数**。 ▍

我们首先研究 $R/(c_i)$ 的进一步的分解。这不外乎是中国剩余定理(定理1.10)的推广。读者请注意，根据定理3.28，主理想整环皆是唯一分解的整环。

定理4.15(中国剩余定理) 设 R 为主理想整环。$c\in R$，c 非零非可逆。设 c 的分解式为

$$c=\delta\prod_{i=1}^{l}p_i^{s_i},$$

其中 δ 可逆，当 $i\neq j$ 时，p_i 与 p_j 不相伴。则恒有下列的 R 模同构：

$$R/(c)\approx R/(p_1^{s_1})\times R/(p_2^{s_2})\times\cdots\times R/(p_l^{s_l}).$$

证明 本定理可遵循定理1.10的证法求得。令

$$d=\delta\prod_{i=2}^{l}p_i^{s_i},\quad c=p_1^{s_1}d.$$

我们证明 $R/(c)\approx R/(p_1^{s_1})\times R/(d)$ 以后，进一步地分解 d，如此反复推论，即可得本定理。

因为 $p_1^{s_1}$ 与 d 无不可逆的公因元，所以有 $(p_1^{s_1},d)=(1)$。即存在 $\alpha,\beta\in R$，使

(1) $$\alpha p_1^{s_1}+\beta d=1.$$

令 σ_1: $R\to R/(p_1^{s_1})$，σ_2: $R\to R/(d)$ 为典型映射。定义模映射

$$\rho:\ R\to R/(p_1^{s_1})\times R/(d),$$

$$\rho(r)=(\sigma_1(r),\sigma_2(r)).$$

我们仅须证明 ρ 是满射及 $\ker(\rho)=(c)$ 便已足够了（参见定理4.9）。

任取 $\sigma_1(r_1)\in R/(p_1^{s_1})$，$\sigma_2(r_2)\in R/(d)$。令

$$r=r_1\beta d+r_2\alpha p_1^{s_1}.$$

根据(1)式，得

$$\sigma_1(r)=\sigma_1(r_1\beta d)=\sigma_1((1-\alpha p_1^{s_1})r_1)=\sigma_1(r_1),$$

$$\sigma_2(r)=\sigma_2(r_2\alpha p_1^{s_1})=\sigma_2((1-\beta d)r_2)=\sigma_2(r_2).$$

即 $\rho(r)=(\sigma_1(r_1),\sigma_2(r_2))$。于是 ρ 是满射。令 $r\in\ker(\rho)$，则有

$$\sigma_1(r)=\bar{0}\Longrightarrow r\in(p_1^{s_1})\Longrightarrow p_1^{s_1}|r,$$

$$\sigma_2(r)=\bar{0}\Longrightarrow r\in(d)\Longrightarrow d|r.$$

因为 $p_1^{s_1}$ 及 d 无不可逆的公因元，所以

$$c=p_1^{s_1}d|r,$$

即 $r\in(c)$。故 $\ker(\rho)\subset(c)$。反之，显然 $(c)\subset\ker(\rho)$，故

$$\ker(\rho)=(c).\ \blacksquare$$

于是，根据定理4.13及定理4.15，我们得出另一种分解如下。

定理4.16 设 R 是一个主理想整环，M 是一个有限生成的 R 模。则存在 R 的元素 $p_1,\cdots,p_q$（其中可能有相同者或相伴者）及正整数 $s_1,\cdots,s_q$，使下列的 R 模为同构：

$$M\simeq\prod_{i=1}^{q}R/(p_i^{s_i})\times R\times\cdots\times R.$$

定理4.13的分解是所谓**挠分解**，定理4.16的分解是**初等分解**，其中相应的 $\{p_1^{s_1},\cdots,p_q^{s_q}\}$ 是**初等因子**。很自然的问题是，给定 R 模 M 以后，这些挠分解、挠因子、初等分解、初等因子等是否唯一确定了呢？答案是肯定的。我们先处理初等分解及初等因

子的问题。令M为

$$\left(\prod_i R/(p_i^{s_i})\right)\times(R\times\cdots\times R),$$

前半部分即M的挠子模N，而$M/N\approx R\times\cdots\times R$是一个自由$R$模。根据定理4.10，这个自由模中含有的$R$的数目$n$（即贝蒂数）是由$M/N$唯一确定的，也即是由$M$唯一确定的。所以问题归结为处理挠子模$N$的问题了。不妨即令

$$N=\prod_i R/(p_i^{s_i}).$$

易于看出$R/(p_i^{s_i})$的消灭子为$(p_i^{s_i})$。我们假定N的初等分解式中诸p_i或者相同，或者不相伴，亦即将相伴的素挠因子都换成同一个。容易证明：这些素元素的集合$\{p_i\}$由N唯一决定。令

$$N_{p_i}=\{n\in N:\ \text{存在正整数}\ k,\ \text{使}\ p_i^k n=0\}.$$

显然N_{p_i}是N的子模，而且，注意到上述的假定，即知

$$N_{p_i}\approx\prod_{p_j=p_i}R/(p_j^{s_j}).$$

于是有下列的模同构

$$N\approx\prod_i N_{p_i}.$$

经过这样的简化以后，问题归结成，对一个固定的素元素p_i（为方便起见，令$p=p_i$），

$$N_p=\prod_{j=1}^{d}(R/(p^{s_j}))$$

可不可能有另一个初等分解？

考虑$(p)N_p$及$N_p/(p)N_p$两个模。不难看出

$$(p)N_p=\prod_{j=1}^{d}(p)R/(p^{s_j})\approx\prod_{j=1}^{d}R/(p^{s_j-1}).$$

上式的同构是这样定义的：令 $R/(p^{s_j})$ 的元素为 $[r]_1$，$R/(p^{s_j-1})$ 的元素为 $[r]_2$，定义 ρ：$R/(p^{s_j-1})\to(p)R/(p^{s_j})$ 为

$$\rho([r]_2)=[pr]_1,$$

读者自证 ρ 确为同构映射。自然的，如果 $s_j=1$，则 $(p^{s_j-1})=R$。对 s_j 采取数学归纳法，根据归纳法假设，知 $(p)N_p$ 的初等分解是唯一确定的。于是 N_p 的初等分解式中 p 的方幂指数集合 $\{s_j\}$ 的子集合 $\{s_j:\ s_j>1\}$ 也是唯一确定的。目前未知的，仅是集合 $\{s_j:\ s_j=1\}$。我们仅须证明 $\{s_j\}$ 的总数 d 是确定的便已足够了。

为此，我们需要证明

(1) $$A\times B/C\times D\approx A/C\times B/D,$$

其中 C 是 A 的子模，D 是 B 的子模；

(2) $$\frac{R/(p^{s_j})}{(p)R/(p^{s_j})}\approx R/(p);$$

(3) $$N_p/(p)N_p\approx R/(p)\times R/(p)\times\cdots\times R/(p),$$

此式右侧共有 d 个 $R/(p)$；

(4) $R/(p)$ 是域，$N_p/(p)N_p$ 是 $R/(p)$ 上的 d 维向量空间。

于是 $\{s_j\}$ 的总数 d 是由 $N_p/(p)N_p$ 确定的，不因初等分解而变。

证明(1)式。我们定义模映射

$$\sigma:\ A\times B\to A/C\times B/D,$$
$$\sigma((a,b))=([a],[b]).$$

易于看出 σ 为一满射，而且 $\ker(\sigma)=C\times D$。根据定理4.9，(1)式得证。

证明(2)式。请注意 $(p^{s_j})\subset(p)$。令 σ_j：$R/(p^{s_j})\to R/(p)$ 定义如下：对于 $[r]_1\in R/(p^{s_j})$，

$$\sigma_j([r]_1)=[r]_2\in R/(p).$$

此映射 σ_j 显然是满射。又有

$$[r]_2=0\Longleftrightarrow r\in(p)\Longleftrightarrow r=pr'\Longleftrightarrow[r]_1=p[r']_1,$$

于是 $\ker(\sigma_j)=(p)R/(p^{s_j})$。根据定理4.9，(2)式得证。

(3)式可自(1)式及(2)式直接导出。(4)式也仅须证明 $R/(p)$

是域。根据定理3.24，即证(p)是极大理想。因为R是主理想整环，如有理想$J\supsetneqq(p)$，取$a\in J\setminus(p)$，则有

$$J\supset(p,a)=(1)=R.$$

所以(4)式也得证。

综上所述，我们有下列的唯一性定理。

定理4.17 在定理4.16的初等分解中，除了变换次序外，M的分解是唯一确定的。

系 一个有限交换群G为循环群的充要条件是：在G初等分解中，所有的p_j皆不相同。

证明 应用中国剩余定理。▎

我们现在来解决挠分解的唯一性的问题。

定理4.18 在定理4.13中，M的挠分解是唯一确定的。

证明 取M的初等因子的集合$\{p_1^{s_1},\cdots,p_q^{s_q}\}$，如果$p_i$与$p_j$相伴，可令其为相同。令$\{p_1,\cdots,p_t\}$为不同的$p_i$的集合。把$\{p_1^{s_1},\cdots,p_q^{s_q}\}$按$\{p_1,\cdots,p_t\}$的次序排成列，按指数的大小排成行如下：

$$\begin{array}{ll}
p_1 & \cdots,\ p_1^{s_{1,l-1}},\ p_1^{s_{1l}},\\
p_2 & \cdots,\ p_2^{s_{2,l-1}},\ p_2^{s_{2l}},\\
\vdots & \cdots\cdots\cdots\cdots\cdots\cdots\\
p_t & \cdots,\ p_t^{s_{t,l-1}},\ p_t^{s_{tl}},
\end{array}$$

其中每行指数是渐增的。在M的挠分解中，

$$\left(\prod_{i=1}^{l}c_i\right)=\left(\prod_{j,r}p_j^{s_{jr}}\right),\qquad c_1|c_2|\cdots|c_l.$$

所以显然易见，(c_l)必为最后一列的连乘积生成的，(c_{l-1})必为倒数第二列连乘积生成的，等等。于是$(c_1),(c_2),\cdots,(c_l)$皆由初等因子所确定，由此得证本定理。▎

例12 试问有几种互不同构的阶数为100的交换群？

根据定理4.16及定理4.17，阶数为100的交换群不外乎

$$\boldsymbol{Z}_{2^2}\times\boldsymbol{Z}_{5^2},\ \ \boldsymbol{Z}_2\times\boldsymbol{Z}_2\times\boldsymbol{Z}_{5^2},\ \ \boldsymbol{Z}_{2^2}\times\boldsymbol{Z}_5\times\boldsymbol{Z}_5,\ \ \boldsymbol{Z}_2\times\boldsymbol{Z}_2\times\boldsymbol{Z}_5\times\boldsymbol{Z}_5$$

四种。一般言之，设 $n=\prod_i p_i^{s_i}$，不难看出，阶数为 n 的交换群有 $\prod_i P(s_i)$ 种，此处 $P(s_j)$ 是 s_j 的划分数，即 s_j 写成正整数和的不同写法的个数。例如

$$1=1 \Longrightarrow P(1)=1;$$

$$2=2,\ 2=1+1 \Longrightarrow P(2)=2;$$

$$3=3,\ 3=1+2,\ 3=1+1+1 \Longrightarrow P(3)=3;$$

$$4=4,\ 4=3+1,\ 4=2+2,\ 4=2+1+1,\ 4=1+1+1+1 \\ \Longrightarrow P(4)=5,$$

等等。例如，$100=2^2\times 5^2$，于是 $P(2)P(2)=2\times 2=4$。

习　题

1．设 M 是 R 模，M 和 R 的零元分别记为 $0_M, 0_R$。证明

(1) $r0_M=0_M$，$\forall r\in R$；

(2) $0_Rm=0_M$，$\forall m\in M$；

(3) $(-r)m=r(-m)=-rm$，$\forall r\in R$，$m\in M$。

2．证明 R 模 M 的任意多个子模的交以及和皆为子模，但子模的并集不一定是子模。

3．证明子模 M 由 $\{m_i: i\in I\}$ 生成 $\Longleftrightarrow M$ 是包含 $\{m_i: i\in I\}$ 的最小子模(此处 I 为一个指标集合)。

4．设 I 是环 R 的理想，证明 I 是 R 模。又若 M 是 R 模，则 IM 是 M 的子模。

5．设 M 是 R 模，N_1, N_2 是 M 的子模。令

$$(N_1: N_2)=\{r\in R: rN_2\subset N_1\},$$

证明 $(N_1:N_2)$ 是 R 的理想。

6．设 R 为整环，证明 R 上的自由模是无挠的。举例说明无挠模不一定是自由模。

7．设 M 是自由 R 模，$\{e_1,e_2,\cdots,e_n\}$ 是 M 的一组 R 基。设有

$\xi_1,\xi_2,\cdots,\xi_n\in M$，满足

$$(\xi_1,\xi_2,\cdots,\xi_n)=(e_1,e_2,\cdots,e_n)A,$$

其中

$$A=\begin{bmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{bmatrix}, \quad a_{ij}\in R.$$

证明$\{\xi_1,\xi_2,\cdots,\xi_n\}$是$M$的$R$基$\Longleftrightarrow \det A$是$R$中的可逆元。

8．设R是环．如果每个自由R模的子模都是自由模，证明R是主理想整环。

9．将向量空间的直和、直积推广到模上。

10．将群的第一、第二、第三同构定理及许来尔定理、若当-荷德定理推广到模上。

11．证明$\mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/2\mathbf{Z}$与$\mathbf{Z}/4\mathbf{Z}$不同构。

12．有多少互不同构的交换群，其阶为12和600？

§5 若当标准式

在本节中，我们要应用上节的定理4.13及定理4.16，以求得一个矩阵的"若当标准式"（请见定理4.25）。本节的主要工作不过是了解及解释上面提到的那两个定理。

参考例11，设K是域，$A\in \mathrm{Hom}_K(K^n,K^n)$，则通过$A$的如下作用，$K^n$成为一个$K[x]$模：

$$f(x)(v)=f(A)(v),\quad \forall f(x)\in K[x],\ v\in K^n.$$

于是定理4.13证明了

$$K^n\approx(K[x]/(c_1(x))\times\cdots\times K[x]/(c_l(x)))\\ \times(K[x]\times\cdots\times K[x]).$$

因为$K[x]$是无限维的K向量空间，而K^n是有限维的K向量空间，于是，上式中的第二个括号必不存在。所以我们有下列二定理：

理。为了简明起见，我们假定诸 $c_i(x)$ 皆为首一多项式（最高次项的系数为 1 的多项式）。事实上，任何非零的多项式，只要乘以适当的常数，皆可化为首一多项式。

定理4.19 设K是域，$A\in \mathrm{Hom}_K(K^n,K^n)$。令 $x\cdot v$ 定义成 $A(v)$，$f(x)\cdot v$ 定义成$f(A)(v)$，$\forall f(x)\in K[x]$。则唯一地存在一组首一多项式 $c_1(x),c_2(x),\cdots,c_l(x)\in K[x]$，使

1) $c_1(x)|c_2(x)|\cdots|c_l(x)$，$\deg c_i(x)\geqslant 1$；

2) $K^n\approx K[x]/(c_1(x))\times K[x]/(c_2(x))\times\cdots\times K[x]/(c_l(x))$。

这些首一多项式 $c_1(x),c_2(x),\cdots,c_l(x)$称为$A$的**不变因子**。

定理4.20 设K是域，$A\in \mathrm{Hom}_K(K^n,K^n)$，将 $x\cdot v$ 定义成 $A(v)$，$f(x)\cdot v$ 定义成 $f(A)(v)$，$\forall f(x)\in K[x]$。则唯一地存在一组不可约的首一多项式 $p_1(x),\cdots,p_q(x)$（其中可能有相同者）及正整数 $s_1,\cdots,s_q$，使

$$K^n\approx\prod_{i=1}^{q}K[x]/(p_i(x)^{s_i})。$$

$\{p_i(x)^{s_i}\}$称为A的**初等因子**。

根据上面的两个定理，A对 K^n 的线性的作用，转化为 x 对 $K[x]/(g(x))$的一般的乘法的作用。

定理 4.21 设 $g(x)=-a_0-a_1x-\cdots-a_{m-1}x^{m-1}+x^m$。则 $K[x]/(g(x))$是m维K 向量空间，并且$\{1,[x],\cdots,[x^{m-1}]\}$是 $K[x]/(g(x))$的一组基。对于这组基，线性变换 x 的矩阵表示式（参考定理4.7）是下列的所谓**不变式的块矩阵**：

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & \cdots & 0 & a_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & a_{n-2} \\ 0 & 0 & 0 & \cdots & 0 & 1 & a_{n-1} \end{pmatrix}.$$

证明 我们先证 $\{1,[x],\cdots,[x^{m-1}]\}$ 是 $K[x]/(g(x))$ 的生成元集。任取 $[f(x)]\in K[x]/(g(x))$。由欧几里得算法，存在 $d(x)$ 及 $r(x)$，使

$$f(x)=d(x)g(x)+r(x),\qquad \deg r(x)<\deg g(x)=m.$$

立得

$$[f(x)]=[d(x)][g(x)]+[r(x)]=[r(x)].$$

$[r(x)]$ 自然可以由 $\{1,[x],\cdots,[x^{m-1}]\}$ 生成。其次，设有

$$\sum_{i=0}^{m-1}a_i[x^i]=0,$$

即

$$\left[\sum_{i=0}^{m-1}a_ix^i\right]=0,\quad \sum_{i=0}^{m-1}a_ix^i\in(g(x)),\qquad g(x)\,\Big|\,\sum_{i=0}^{m-1}a_ix^i.$$

故 $a_i=0$，$\forall i=0,1,\cdots,m-1$。于是 $\{1,[x],\cdots,[x^{m-1}]\}$ 是线性无关集。因此，$\{1,[x],\cdots,[x^{m-1}]\}$ 是一组基，$K[x]/(g(x))$ 是 m 维线性空间。

我们具体地写出 x 在 $K[x]/(g(x))$ 上的线性作用：

$$x(1)=[x\times1]=0\times1+[x]+0\times[x^2]+\cdots+0\times[x^{m-1}],$$

$$\begin{aligned}x([x])&=[x\times x]\\&=0\times1+0\times[x]+[x^2]+0\times[x^3]+\cdots+0\times[x^{m-1}],\end{aligned}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$x([x^{m-1}])=[x\times x^{m-1}]=[x^m]=a_0+a_1[x]+\cdots+a_{m-1}[x^{m-1}].$$

取出上述各方程的系数，再将行列调换，即得我们所要的矩阵。▌

于是，我们有下列关于“不变式”的定理。

定理4.22 设 K 是域，$A\in\mathrm{Hom}_K(K^n,K^n)$。则适当地选取 K^n 的基以后，A 的矩阵表示式可以成为如下的所谓**不变式**，其

中对角线上皆是不变式的块矩阵(见定理4.21):

$$\begin{bmatrix} B_1 & & & \\ & B_2 & & 0 \\ 0 & & \ddots & \\ & & & B_l \end{bmatrix}.$$

而两个矩阵相似的充要条件是：它们的不变式最多只能有对角线上块矩阵次序的差异。

证明 不变式的存在性，可以直接从定理4.19及定理4.21导出。

关于本定理的后半部分，其充分性是显然的，因为矩阵与其不变式是相似的，而相似关系是一个等价关系。我们证明必要性。设A与B相似，则A与B可以看成同一线性变换T对不同基的矩阵表示式。显然的，K^n通过A和B的作用得出的两个$K[x]$模是同构的。根据定理4.19的唯一性，即知两者的不变式最多只能有对角线上块矩阵次序的差异。 ∎

设K是复数域C(一般言之，可设域K是"代数封闭的"，详情请见下一章)，则定理4.20给出矩阵A的一个简单的"若当标准式"(详见下面的讨论)。我们要用到复数域C的一个极重要的性质，即下面的定理。其证明在下一章的§1。

定理4.23(代数基本定理) $C[x]$中的不可约的多项式皆是一次多项式。

上面这个定理意即$C[x]$中每一个次数大于零的多项式$f(x)$在C中均有解。这因为$f(x)$可分解成不可约多项式的乘积

$$f(x) = \prod_i (a_i x - b_i),$$

于是$x = b_i/a_i$即其解。应用定理4.20及定理4.23，即可得出

定理4.24 上述的$\{1, [x-c], [(x-c)^2], \cdots, [(x-c)^{m-1}]\}$是$K[x]/((x-c)^m)$的一组基。相对于这组基，线性变换$x$的矩阵

表示式是如下的若当标准式块矩阵，

$$\begin{bmatrix} c & & & & 0 \\ 1 & c & & & \\ & 1 & c & & \\ & & \ddots & \ddots & \\ 0 & & & 1 & c \end{bmatrix}.$$

证明 显然有

$$\sigma(1)=c\times 1+1\times[x-c]+0\times[(x-c)^2]+\cdots+0\times[(x-c)^{m-1}],$$

$$\sigma([x-c])=0\times 1+c\times[x-c]+1\times[(x-c)^2]+\cdots+0\times[(x-c)^{m-1}],$$

$$\cdots\cdots$$

$$\sigma([(x-c)^{m-2}])=0\times 1+0\times[x-c]+\cdots+c\times[(x-c)^{m-2}]+1\times[(x-c)^{m-1}],$$

$$\sigma([(x-c)^{m-1}])=0\times 1+0\times[x-c]+\cdots+0\times[(x-c)^{m-2}]+c\times[(x-c)^{m-1}].$$

取出其系数即得本定理。 ▎

定理4.25(若当标准式) 设$A\in \mathrm{Hom}_K(K^n,K^n)$。如果$A$的不变因子$c_1(x),c_2(x),\cdots,c_l(x)$皆可在$K[x]$中分解成一次式的乘积(例如$K=\boldsymbol{C}$，以上条件是自然成立的)，则适当地选取$K^n$的基以后，$A$的矩阵表示式可成为如下的**若当标准式**，其中对角线上皆是若当标准式的块矩阵(见定理4.24)：

$$\begin{bmatrix} J_1 & & & 0 \\ & J_2 & & \\ & & \ddots & \\ 0 & & & J_m \end{bmatrix}.$$

如果$K=\boldsymbol{C}$，那末两个矩阵相似的充要条件是：它们的若当标准式最多只能有对角线上块矩阵次序的差异。

证明 仿照定理4.22的证法，读者补充完成之。 ▎

设域K是实数域$\boldsymbol{R}$。$\boldsymbol{R}[x]$中的不可约的首一多项式是一次多项式$(x-a)$或二次多项式$(x-a)^2+b^2(b\neq 0)$。其证法可自代数基本定理导出，详情请见下一章。这里我们暂时先应用这个事

实，以得出实数的若当标准式。

定理4.26 给定 $a,b\in\boldsymbol{R}$，$b\neq 0$。定义 $F(n)\in\boldsymbol{C}[x]$，$G(n)$，$H(n)\in\boldsymbol{R}[x]$ 如下：

$$F(n)=[(x-a)+b\mathrm{i}]^{n}=G(n)+\mathrm{i}H(n),\quad n=1,2,\cdots.$$

令

$$\triangle=(x-a)^{2}+b^{2}.$$

又设 m 是一正整数，对 $n=1,2,\cdots,m$，令

$$v_{2m-2n+2}=[G(n)+H(n)]\triangle^{m-n},$$

$$v_{2m-2n+1}=[G(n)-H(n)]\triangle^{m-n}.$$

则 $\{v_1,v_2,\cdots,v_{2m}\}$ 是 $\boldsymbol{R}[x]/(\triangle^{m})$ 的一组基。线性变换 x 在这组基下的矩阵表示式是如下的实数的若当标准式的块矩阵：

$$\begin{bmatrix} a & b & & & & & & \\ -b & a & & & & & \multicolumn{2}{c}{0} \\ 1 & 0 & a & b & & & & \\ 0 & 1 & -b & a & & & & \\ & & \ddots & \ddots & \ddots & & & \\ & 0 & & 1 & 0 & a & b & \\ & & & 0 & 1 & -b & a & \end{bmatrix}.$$

证明　我们先假设 $\{v_1,v_2,\cdots,v_{2m}\}$ 是 $\boldsymbol{R}[x]/(\triangle^{m})$ 的一组基，完成了定理后半部分的证明。

我们先证明几个多项式的恒等式。考虑

$$\begin{aligned}(x-a)F(n)&=[(x-a)+b\mathrm{i}]^{n+1}-b\mathrm{i}[(x-a)+b\mathrm{i}]^{n}\\&=[G(n+1)+bH(n)]+\mathrm{i}[H(n+1)-bG(n)],\end{aligned}$$

于是有

(1)　　$$(x-a)G(n)=G(n+1)+bH(n),$$

(2)　　$$(x-a)H(n)=H(n+1)-bG(n).$$

又考虑

$$F(n+1)=[G(n-1)+\mathrm{i}H(n-1)][(x-a)^{2}+2b(x-a)\mathrm{i}-b^{2}]$$

$$=[G(n-1)+iH(n-1)]\triangle$$
$$+2bi[G(n-1)+iH(n-1)](x-a+bi)$$
$$=[G(n-1)+iH(n-1)]\triangle+2bi[G(n)+iH(n)],$$

于是有

(3) $$G(n+1)=G(n-1)\triangle-2bH(n),$$

(4) $$H(n+1)=H(n-1)\triangle+2bG(n).$$

计算下式时，以(1),(2),(3),(4)式适当地代入，有

(5) $$(x-a)v_{2m-2n+2}=[(x-a)G(n)+(x-a)H(n)]\triangle^{m-n}$$
$$=[G(n+1)+H(n+1)-2bG(n)$$
$$+2bH(n)]\triangle^{m-n}+bv_{2m-2n+1}$$
$$=v_{2m-2n+4}+bv_{2m-2n+1},$$

(6) $$(x-a)v_{2m-2n+1}=v_{2m-2n+3}-bv_{2m-2n+2}.$$

在(5)及(6)式中，如果 $n=1$，则

$$v_{2m-2n+4}=v_{2m-2n+3}=\triangle^{m}=\bar{0}\in \boldsymbol{R}[x]/(\triangle^{m}).$$

由(5)及(6)式，即有

$$\begin{aligned}
x(v_1)&=av_1-bv_2+v_3,\\
x(v_2)&=av_1+bv_2+v_4,\\
x(v_3)&=av_3-bv_4+v_5,\\
x(v_4)&=bv_3+av_4+v_6,\\
&\cdots\cdots\\
x(v_{2m-1})&=av_{2m-1}-bv_{2m},\\
x(v_{2m})&=bv_{2m-1}+av_{2m}.
\end{aligned}$$

于是取出其系数，排成矩阵，行列调置，即得本定理的后半部分。

我们现在证明$\{v_1,v_2,\cdots,v_{2m}\}$确是$\boldsymbol{R}[x]/(\triangle^m)$的基。注意到$\boldsymbol{R}[x]/(\triangle^m)$是 $2m$ 维实向量空间，而集合$\{v_i\}$中确有$2m$个元素，所以，如果$\{v_i\}$不是基，则必线性相关，即存在不全为零的 $a_1,\cdots,a_{2m}\in\boldsymbol{R}$，使

$$\sum_i a_i v_i = \bar{\bar{0}} \Longleftrightarrow \sum_i a_i v_i \in (\triangle^m)$$

$$\Longleftrightarrow \sum_i a_i v_i = g(x)\triangle^m \qquad (g(x) \in \mathbf{R}[x])$$

$$\Longrightarrow \sum_i a_i v_i = g(x)\triangle^m \qquad (g(x) \in \mathbf{C}[x])$$

$\Longleftrightarrow \{v_1, \cdots, v_{2m}\}$ 在 $\mathbf{C}[x]/(\triangle^m)$中的象是线性相关的。

我们仅须对最后一个命题找出矛盾即可。

因为 $\mathbf{C}[x]/(\triangle^m)$是$2m$ 维复向量空间，所以，我们只要证明出$\{v_1, \cdots, v_{2m}\}$是 $\mathbf{C}[x]/(\triangle^m)$的生成元集，即知其必为基，也就找出所需要的矛盾。

令 $c = a + b\mathrm{i}$，$\bar{c} = a - b\mathrm{i}$。显然有

$$\triangle = (x-c)(x-\bar{c}),$$

$$\frac{1}{2}(v_{2m-2n+2} + v_{2m-2n+1}) + \frac{1}{2}\mathrm{i}(v_{2m-2n+2} - v_{2m-2n+1})$$
$$= F(n)\triangle^{m-n}$$
$$= (x-\bar{c})^n (x-c)^{m-n} (x-\bar{c})^{m-n} = (x-\bar{c})^m (x-c)^{m-n},$$

$$\frac{1}{2}(v_{2m-2n+2} + v_{2m-2n+1}) - \frac{1}{2}\mathrm{i}(v_{2m-2n+2} - v_{2m-2n-1})$$
$$= (G(n) - \mathrm{i}H(n))\triangle^{m-n}$$
$$= (x-c)^n (x-c)^{m-n} (x-\bar{c})^{m-n} = (x-c)^m (x-\bar{c})^{m-n}.$$

于是由$\{v_1, \cdots, v_{2m}\}$生成的子空间V中含有

$$\{(x-\bar{c})^m, (x-c)(x-\bar{c})^m, \cdots, (x-c)^{m-1}(x-\bar{c})^m,$$
$$(x-c)^m, (x-\bar{c})(x-c)^m, \cdots, (x-\bar{c})^{m-1}(x-c)^m\},$$

这些元素分别记为 $u_1, u_2, \cdots, u_m, w_1, w_2, \cdots, w_m$。我们要证明$\{u_1, u_2, \cdots, u_m, w_1, w_2, \cdots, w_m\}$生成$\mathbf{C}[x]/(\triangle^m)$，如此便证明了本定理。

考虑如下的环同构(参考中国剩余定理，即定理4.15)：

$$\rho: \mathbf{C}[x]/(\triangle^m) \approx \mathbf{C}[x]/((x-c)^m) \times \mathbf{C}[x]/((x-\bar{c})^m).$$

因为$(x-\bar{c})^m$与$(x-c)^m$无不可逆的公因元（因$b\neq0$），所以存在$\alpha(x),\beta(x)\in \boldsymbol{C}[x]$，使

$$\alpha(x)(x-c)^m+\beta(x)(x-\bar{c})^m=1.$$

所以$(x-c)^m$在环$\boldsymbol{C}[x]/((x-c)^m)$中的象是零，以及$(x-c)^m$在环$\boldsymbol{C}[x]/((x-\bar{c})^m)$中的象是可逆的。于是，由任何如下的线性关系

$$\sum_{j=1}^{m} a_j\rho(w_j)=0$$

立得在$\boldsymbol{C}[x]/((x-\bar{c})^m)$内

$$\sum_{j=0}^{m-1} a_{j+1}(x-\bar{c})^j=0.$$

而$(x-\bar{c})^j$是j次式，故$\{\rho(x-\bar{c})^j:\ j=0,1,\cdots,m-1\}$是$\boldsymbol{C}$向量空间$\boldsymbol{C}[x]/((x-\bar{c})^m)$的一组基，所以上式的诸$a_{j+1}(j=0,1,\cdots,m-1)$必全为零，这就证明了$\{\rho(w_j):\ j=1,2,\cdots,m\}$是$\{0\}\times\boldsymbol{C}[x]/((x-\bar{c})^m)$的线性无关集，也即生成元集。同法可证$\{\rho(u_j):\ j=1,2,\cdots,m\}$是$\boldsymbol{C}[x]/((x-c)^m)\times\{0\}$的生成元集。综上所述，$\{u_1,\cdots,u_m,w_1,\cdots,w_m\}$是$\boldsymbol{C}[x]/(\triangle^m)$的生成元集。 ▎

定理4.27 设$A\in \mathrm{Hom}_{\boldsymbol{R}}(\boldsymbol{R}^n,\boldsymbol{R}^n)$。则适当地选取$\boldsymbol{R}^n$的基以后，$A$的矩阵表示式可成为如下的**实数若当标准式**，其中对角线上皆是若当标准式的块矩阵（见定理4.24（其中$c\in\boldsymbol{R}$)及定理4.26)：

$$\begin{bmatrix} J_1 & & & 0 \\ & J_2 & & \\ & & \ddots & \\ 0 & & & J_n \end{bmatrix}.$$

而且两个矩阵相似的充要条件是：它们的实数若当标准式最多只能有对角线上块矩阵次序的差异。

证明 仿照定理4.22的证法，读者补充完成之。 ▎

例13 解一阶常微分方程组(参考例8)。为简便起见，取四

个实函数的例子，

(1)
$$\begin{cases}\dfrac{df_1}{dx}=a_{11}f_1+a_{12}f_2+a_{13}f_3+a_{14}f_4,\\ \dfrac{df_2}{dx}=a_{21}f_1+a_{22}f_2+a_{23}f_3+a_{24}f_4,\\ \dfrac{df_3}{dx}=a_{31}f_1+a_{32}f_2+a_{33}f_3+a_{34}f_4,\\ \dfrac{df_4}{dx}=a_{41}f_1+a_{42}f_2+a_{43}f_3+a_{44}f_4.\end{cases}$$

或写成矩阵式

(2)
$$\frac{d}{dx}\begin{bmatrix}f_1\\f_2\\f_3\\f_4\end{bmatrix}=A\begin{bmatrix}f_1\\f_2\\f_3\\f_4\end{bmatrix}.$$

根据定理4.27，存在矩阵B及A'，使

(3) A'是A的实数若当标准式，

(4) $$A=BA'B^{-1}.$$

令

(5)
$$B^{-1}\begin{bmatrix}f_1\\f_2\\f_3\\f_4\end{bmatrix}=\begin{bmatrix}g_1\\g_2\\g_3\\g_4\end{bmatrix},\quad \begin{bmatrix}f_1\\f_2\\f_3\\f_4\end{bmatrix}=B\begin{bmatrix}g_1\\g_2\\g_3\\g_4\end{bmatrix}.$$

则以(4)式代入(2)式后，两侧乘以B^{-1}，得

(6)
$$\frac{d}{dx}\begin{bmatrix}g_1\\g_2\\g_3\\g_4\end{bmatrix}=A'\begin{bmatrix}g_1\\g_2\\g_3\\g_4\end{bmatrix}.$$

解出(6)式，代入(5)式，即得到f_1,f_2,f_3,f_4。根据定理4.27，

(6)式中的A'基本上只有下列几种可能：

$$\begin{bmatrix} r_1 & & & 0 \\ & r_2 & & \\ & & r_3 & \\ 0 & & & r_4 \end{bmatrix}, \begin{bmatrix} r_1 & 0 & & 0 \\ 1 & r_1 & & \\ & 0 & r_2 & 0 \\ & & 0 & r_3 \end{bmatrix}, \begin{bmatrix} r_1 & 0 & & 0 \\ 1 & r_1 & & \\ & 0 & r_2 & 0 \\ & & 1 & r_2 \end{bmatrix},$$

$$\begin{bmatrix} r_1 & 0 & 0 & \\ 1 & r_1 & 0 & 0 \\ 0 & 1 & r_1 & \\ & 0 & & r_2 \end{bmatrix}, \begin{bmatrix} r_1 & 0 & 0 & 0 \\ 1 & r_1 & 0 & 0 \\ 0 & 1 & r_1 & 0 \\ 0 & 0 & 1 & r_1 \end{bmatrix}, \begin{bmatrix} a & b & & 0 \\ -b & a & & \\ & 0 & r_1 & 0 \\ & & 0 & r_2 \end{bmatrix},$$

$$\begin{bmatrix} a & b & & 0 \\ -b & a & & \\ & 0 & r_1 & 0 \\ & & 1 & r_1 \end{bmatrix}, \begin{bmatrix} a_1 & b_1 & & 0 \\ -b_1 & a_1 & & \\ & 0 & a_2 & b_2 \\ & & -b_2 & a_2 \end{bmatrix}, \begin{bmatrix} a & b & & 0 \\ -b & a & & \\ 1 & 0 & a & b \\ 0 & 1 & -b & a \end{bmatrix}.$$

我们试以最后一个矩阵为例求解.

$$\frac{\mathrm{d}}{\mathrm{d}x}\begin{bmatrix} g_1 \\ g_2 \\ g_3 \\ g_4 \end{bmatrix} = \begin{bmatrix} a & b & 0 & 0 \\ -b & a & 0 & 0 \\ 1 & 0 & a & b \\ 0 & 1 & -b & a \end{bmatrix}\begin{bmatrix} g_1 \\ g_2 \\ g_3 \\ g_4 \end{bmatrix},$$

即

$$(1')\qquad \frac{\mathrm{d}}{\mathrm{d}x}g_1 = ag_1 + bg_2,$$

$$(2')\qquad \frac{\mathrm{d}}{\mathrm{d}x}g_2 = -bg_1 + ag_2,$$

$$(3')\qquad \frac{\mathrm{d}}{\mathrm{d}x}g_3 = g_1 + ag_3 + bg_4,$$

$$(4')\qquad \frac{\mathrm{d}}{\mathrm{d}x}g_4 = g_2 - bg_3 + ag_4.$$

用复变函数的方法求解方程式(1′),(2′)。令

$$h_1 = g_1 + \mathrm{i}g_2, \quad h_2 = g_1 - \mathrm{i}g_2 = \bar{h}_1,$$

于是有

$$\frac{\mathrm{d}}{\mathrm{d}x}h_1 = (a - b\mathrm{i})h_1, \quad \frac{\mathrm{d}}{\mathrm{d}x}h_2 = (a + b\mathrm{i})h_2.$$

其解如下(k为复数)

$$h_1 = k\mathrm{e}^{(a-b\mathrm{i})x} = k(\mathrm{e}^{ax}\cos bx - \mathrm{i}\mathrm{e}^{ax}\sin bx),$$

$$h_2 = \bar{k}(\mathrm{e}^{ax}\cos bx + \mathrm{i}\mathrm{e}^{ax}\sin bx).$$

解之得g_1, g_2(c_1, c_2为实数)

$$g_1 = c_1\mathrm{e}^{ax}\cos bx + c_2\mathrm{e}^{ax}\sin bx,$$

$$g_2 = c_1\mathrm{e}^{ax}\cos bx - c_2\mathrm{e}^{ax}\sin bx.$$

在解(3′),(4′)时，用“变化系数法”，即在(3′),(4′)式中先忽略g_1, g_2，对g_3, g_4求解，解法如上。然后令其系数——即 c_3, c_4，见下式——为函数，代入(3′)及(4′)式中求解c_3及c_4:

$$(3'') \quad \frac{\mathrm{d}}{\mathrm{d}x}(c_3(x)\mathrm{e}^{ax}\cos bx + c_4(x)\mathrm{e}^{ax}\sin bx) = g_1 + ag_3 + bg_4,$$

$$(4'') \quad \frac{\mathrm{d}}{\mathrm{d}x}(c_3(x)\mathrm{e}^{ax}\cos bx - c_4(x)\mathrm{e}^{ax}\sin bx) = g_2 - bg_3 + ag_4.$$

化简后，立得

$$\frac{\mathrm{d}}{\mathrm{d}x}c_3(x) = c_1, \quad \frac{\mathrm{d}}{\mathrm{d}x}c_4(x) = c_2.$$

解之得

$$c_3(x) = c_1x + c_1', \quad c_4(x) = c_2x + c_2'.$$

上式的 c_1, c_2, c_1', c_2' 皆是实数。上面用的这个方法，并不难懂.读者可以系统化地加以推广。

于是，解一阶常微分方程组的问题归结为解(4)式以求矩阵 B 的问题。▌

映射σ: $K[x] \to K[A]$($\sigma(x) = A$)的核

$$\ker(\sigma) = \{f(x): f(x) \in K[x], f(A) = 0\}$$

显然是 $K[x]$ 的理想。因为$K[x]$ 是主理想环，所以，$\ker(\sigma) =$

$(g(x))$. 我们定义A的极小多项式为生成$\ker(\sigma)$的首一多项式。设A的极小多项式是$g(x)$，则立得

$$f(A)=0\Longrightarrow f(x)\in\ker(\sigma)\Longrightarrow g(x)\mid f(x).$$

定理4.28 设$A\in\mathrm{Hom}_K(K^n,K^n)$。则$A$的极小多项式等于$A$的最后一个不变因子$c_l(x)$（参考定理4.19）。

证明 用定理4.19的符号。A对K^n的作用同等于x对

$$K[x]/(c_1(x))\times\cdots\times K[x]/(c_l(x))$$

的作用。因为

$$c_1(x)\mid c_2(x)\mid\cdots\mid c_l(x),$$

所以$c_l(x)$作用在$K[x]/(c_j(x))$($j=1,2,\cdots,l$)上皆等于0线性映射，也即$c_l(x)$作用在$K[x]/(c_1(x))\times\cdots\times K[x]/(c_l(x))$上为0。于是我们得知$c_l(A)$作用在$K^n$上为0。这就是说

$$c_l(x)\in\ker(\sigma).$$

反之，设$f(A)$作用在K^n上为0，则$f(x)$作用在

$$K[x]/(c_1(x))\times\cdots\times K[x]/(c_l(x))$$

上为0。特别是$f(x)$作用在$K[x]/(c_l(x))$上为0。于是

$$f(x)\times 1=\bar{0}\in K[x]/(c_l(x)),$$

即$f(x)\in(c_l(x))$。我们已设$c_1(x),\cdots,c_l(x)$均为首一多项式，于是$c_l(x)$即为A的极小多项式。▎

特别良好的矩阵是选取适当的基后，它成为如下的对角矩阵：

$$\begin{bmatrix} a_1 & & & 0 \\ & a_2 & & \\ & & \ddots & \\ 0 & & & a_n \end{bmatrix}.$$

根据若当标准式的唯一性可知这种良好的矩阵的若当标准式就是对角矩阵。我们试回想导出若当标准式的过程：1）求出矩阵的不变因子（定理4.19）；2）把矩阵的不变因子$c_j(x)$进一步分解成$(x-c)^r$的乘积，由此得出初等因子$(x-c)^r$；3）在与每个初等

因子相应的子空间中，选取一组适当的基，使矩阵成为若当标准式的块矩阵；4) 综合上面三点，得出矩阵的若当标准式。不难看出，矩阵的若当标准式是对角矩阵的充要条件是：$c_j(x)(j=1,2,\cdots,l)$皆可分解成一次多项式的乘积且无重根。因为$c_j(x)\mid c_l(x)$，所以立得：

定理4.29 一矩阵A与对角矩阵相似的充要条件是：其极小多项式$c_l(x)$可分解成一次多项式的乘积而且无重根。

系 设$K=\mathbf{C}$。如果$A^m=I$（I为幺矩阵），则A可以对角化。

证明 $x^m-1\in\ker(\sigma)$，所以$c_l(x)\mid x^m-1$，但x^m-1无重根，所以$c_l(x)$无重根。 ▎

我们要用到一个矩阵A的行列式$\det A$，其定义如下：设

$$A=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix},$$

则

$$\det A=\sum \operatorname{Sg}(i_1,\cdots,i_n)a_{1i_1}a_{2i_2}\cdots a_{ni_n},$$

其中

$$\operatorname{Sg}(i_1,\cdots,i_n)=\begin{cases} 0, & \text{如果} i_1,\cdots,i_n \text{有相同者}, \\ 1, & \text{如果}(i_1,\cdots,i_n)\text{是偶变换}, \\ -1, & \text{如果}(i_1,\cdots,i_n)\text{是奇变换}. \end{cases}$$

关于“偶变换”及“奇变换”请见定义2.22.以上行列式$\det A$的定义与A为实数矩阵时的定义完全相同。我们同样有下列的恒等式：

$$\det(AB)=(\det A)(\det B).$$

其证明留给读者。

定义4.15 设$A\in \operatorname{Hom}_K(K^n,K^n)$。则$A$的特征多项式定义为$\det(xI-A)$，此处$I$为幺矩阵。设$V$是$n$维$K$向量空间，$T\in$

$\mathrm{Hom}_K(V,V)$，则T的任一矩阵表示式的特征多项式称为T 的**特征多项式**（参看下定理）。

定理4.30 两相似矩阵的特征多项式必相等，即

$$\det(xI-A)=\det(xI-BAB^{-1}).$$

证明
$$\begin{aligned}\det(xI-BAB^{-1})&=\det(B(xI-A)B^{-1})\\&=(\det B)\det(xI-A)(\det B^{-1})\\&=\det(BB^{-1})\det(xI-A)=\det(xI-A).\end{aligned}$$ ▎

A的特征多项式与A的不变因子的关系如下。

定理4.31 设A的不变因子为 $c_1(x),c_2(x),\cdots,c_l(x)$，则$A$的特征多项式

$$\det(xI-A)=c_1(x)c_2(x)\cdots c_l(x).$$

证明 根据定理4.30，不妨设A为其不变式(参考定理4.22)：

$$A=\begin{bmatrix}B_1 & & & 0\\ & B_2 & & \\ & & \ddots & \\ 0 & & & B_l\end{bmatrix}.$$

则有

$$\det(xI-A)=\prod_{j=1}^{l}\det(xI-B_j).$$

我们仅须证明不变式的块矩阵B_j的特征多项式是$c_j(x)$就足够了。

设$B=B_j$为不变式块矩阵，

$$c_j(x)=-a_0-a_1x-\cdots-a_{m-1}x^{m-1}+x^m.$$

则

$$B=\begin{pmatrix}0 & \cdots & \cdots & 0 & a_0\\ 1 & 0 & \cdots & 0 & a_1\\ & \ddots & \ddots & \vdots & \vdots\\ & & \ddots & 0 & a_{m-2}\\ 0 & & & 1 & a_{m-1}\end{pmatrix}.$$

将$\det(xI-B)$的第二行乘以x加到第一行上，第三行乘以x^2加到

第一行上，…，第m行乘以x^{m-1}加到第一行上，得

$$\det(xI-B)=\begin{vmatrix} 0 & 0 & 0 & \cdots & 0 & c_j(x) \\ -1 & x & 0 & \cdots & 0 & -a_1 \\ & -1 & x & \cdots & \vdots & \vdots \\ & & \ddots & \ddots & \vdots & \vdots \\ & 0 & & \ddots & x & -a_{m-2} \\ & & & & -1 & x-a_{m-1} \end{vmatrix}.$$

按照第一行展开行列式，立得

$$\det(xI-B)=c_j(x). \blacksquare$$

系 设$f(x)=\det(xI-A)$为A的特征多项式，$g(x)$为A的极小多项式，则$g(x)|f(x)$，$f(A)=0$，$f(x)$的根皆是$g(x)$的根。

证明 我们仅证明最后的部分。因为

$$f(x)=\prod_{j=1}^{l}c_j(x),$$

而且$c_1(x)|c_2(x)|\cdots|c_l(x)=g(x)$，所以$f(x)$的根皆是$g(x)$的根。$\blacksquare$

定义4.16 设$A\in \mathrm{Hom}_K(K^n,K^n)$。则$A$的特征多项式$\det(xI-A)$的根称为$A$的**特征根**或**特征值**。

为了阐明特征値的几何意义，我们给出下述的行列式的基本性质：

定理4.32 设$A\in \mathrm{Hom}_K(K^n,K^n)$。则$A$是$K^n$的自同构（即单满线性映射）的充要条件是$\det A\neq 0$。

证明 $\Longrightarrow$。设A是K^n的自同构，不难看出其逆映射A^{-1}也是线性的。于是有

$$1=\det I=\det(AA^{-1})=(\det A)(\det A^{-1}).$$

所以$\det A\neq 0$。

$\Longleftarrow$。设A不是K^n的自同构，因为（参考定理4.9）

$$\dim K^n=\dim\ker(A)+\dim\operatorname{im}(A),$$

所以A如果是单射(即$\ker(A)=\{0\}$)，则必为满射(即$\mathrm{im}(A)=K^n$)。反之亦然。于是A既不是单射，也不是满射。即有一$v_1\in K^n$，使$v_1\neq 0$，但$Av_1=0$。将v_1扩充成K^n的一组基$\{v_1,v_2,\cdots,v_n\}$。则相应于这组基，K^n的自同构A有如下的矩阵表示式

$$C=\begin{bmatrix} 0 & * & \cdots & * \\ 0 & * & \cdots & * \\ \cdots & \cdots & \cdots & \cdots \\ 0 & * & \cdots & * \end{bmatrix}.$$

因为A与C是相似的，故有矩阵B存在，使$A=BCB^{-1}$，故

$$\det A=(\det B)(\det C)(\det B^{-1})=\det C=0. \quad \blacksquare$$

于是我们有如下的关于特征值的定理。

定理4.33 设$A\in \mathrm{Hom}_K(K^n,K^n)$。一常数$\lambda_0\in K$是特征值的充要条件是：存在一非零向量$v\in K^n$，使

$$Av=\lambda_0 v.$$

这样的向量称为(特征值λ_0的)**特征向量**。

证明 $\Longrightarrow$。设λ_0为A的特征值，则有

$$\det(\lambda_0 I-A)=0.$$

按照上一定理，我们知道$\lambda_0 I-A$不是K^n的自同构，所以$\lambda_0 I-A$不是单射(参看上一定理的证明)。于是

$$\ker(\lambda_0 I-A)\neq\{0\}.$$

任取$0\neq v\in\ker(\lambda_0 I-A)$，则有$(\lambda_0 I-A)v=0$，即$\lambda_0 Iv=Av$，亦即$Av=\lambda_0 v$。

$\Longleftarrow$。设有$v\neq 0$，使$Av=\lambda_0 v$，故

$$(\lambda_0 I-A)v=0,$$

即

$$0\neq v\in\ker(\lambda_0 I-A),$$

也即$\lambda_0 I-A$不是单射。按照上一定理，立得

$$\det(\lambda_0 I-A)=0,$$

即λ_0是A的特征值。$\blacksquare$

设$\lambda_0\in K$是A的特征值，则

$$\{v:\ v\in V,\ Av=\lambda_0 v\}$$

是V的一个非零的子空间，称为 λ_0 的**特征子空间**，记为 V_{λ_0}。我们将 $\dim V_{\lambda_0}$的维数称为特征值 λ_0 的**几何次数**。不难看出，如果$(x-\lambda_0)|c_j(x)$，令

$$c_j(x)=(x-\lambda_0)^m p(x),\qquad p(\lambda_0)\neq 0,$$

则有

$$K[x]/(c_j(x))\approx K[x]/((x-\lambda_0)^m)\times K[x]/(p(x)).$$

而 x 对$K[x]/((x-\lambda_0)^m)$的作用，按照定理4.24，有下列的矩阵表示式

$$\begin{bmatrix}\lambda_0 & & & \\ 1 & \lambda_0 & & 0 \\ & \ddots & \ddots & \\ 0 & & 1 & \lambda_0\end{bmatrix},$$

其特征子空间是一维的。于是得出

$$\dim V_{\lambda_0}=\{j:\ (x-\lambda_0)|c_j(x)\}\text{的基数}.$$

另一方面，λ_0作为特征多项式$\det(xI-A)$的根的重数称为λ_0的**代数次数**。于是我们有

$$\lambda_0\text{的几何次数}\leqslant\lambda_0\text{的代数次数}.$$

综上所述，我们立得：

定理4.34 设$A\in\mathrm{Hom}_K(K^n,\ K^n)$，则$A$可以对角化（即$A$相似于一对角矩阵）的充要条件是：所有特征根的几何次数之和等于n，即

$$\sum_{\lambda_0}\dim V_{\lambda_0}=n. \ \blacksquare$$

设$A\in\mathrm{Hom}_K(K^n,K^n)$，$f(x)$为$A$的特征多项式。设

$$f(x)=x^n-a_1x^{n-1}+\cdots+(-1)^n a_n,$$

则其系数a_1与a_n可以解释如下：

$$(-1)^n a_n = f(0) = \det(0 \times I - A) = (-1)^n \det A,$$

即a_n是A的行列式。又令

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix},$$

则

$$\det(xI - A) = \begin{vmatrix} x-a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x-a_{22} & \cdots & -a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ -a_{n1} & -a_{n2} & \cdots & x-a_{nn} \end{vmatrix}.$$

将$\det(xI - A)$展开后，立得

$$a_1 = a_{11} + a_{22} + \cdots + a_{nn}.$$

上式右侧称为矩阵A的迹。从上面的讨论中，我们知道两个相似矩阵有相同的特征多项式，所以必有相同的迹及行列式。

例14 设A为$\mathbf{R}^3$的以原点为心的旋转。显然$A \in \mathrm{Hom}_K(\mathbf{R}^3, \mathbf{R}^3)$。其特征多项式$\det(xI - A)$是三次多项式，所以必有一实根$\lambda_0$。于是有一个$\lambda_0$的特征向量$v$，即

$$Av = \lambda_0 v.$$

v决定的直线即是A的旋转轴（参考第二章§3的例10，在那里我们假定了$\mathbf{R}^3$的旋转皆有旋转轴，而没有给出证明）。同法立得，$\mathbf{R}^{2n+1}$的旋转皆有旋转轴。一般言之，$\mathbf{R}^{2n}$的旋转不一定有旋转轴。

习　题

1. 找出下列矩阵的初等因子、不变因子、极小多项式：

$$(1)\begin{bmatrix} 1 & 2 & 0 \\ 0 & 2 & 0 \\ -2 & -2 & -1 \end{bmatrix};\qquad (2)\begin{bmatrix} 1 & -1 & 2 \\ 3 & -3 & 6 \\ 2 & -2 & 4 \end{bmatrix}.$$

2. 将下列矩阵化为若当标准式：

$$(1)\begin{bmatrix} 4 & 5 & -2 \\ -2 & -2 & 1 \\ -1 & -1 & 1 \end{bmatrix};\qquad (2)\begin{bmatrix} 1 & -i & i \\ i & 2 & 2 \\ -i & -2 & 2 \end{bmatrix}.$$

3. 找出3×3矩阵A，使

$$A\begin{bmatrix} 5 & 4 & 3 \\ -1 & 0 & -3 \\ 1 & -2 & 1 \end{bmatrix}A^{-1}$$

成若当标准式。

4. 证明下列三个有理矩阵对有理数域$\mathbf{Q}$是相似的(即它们之间的相似演化矩阵可以是有理矩阵)：

$$\begin{bmatrix} 0 & 1 & 0 \\ 4 & 0 & 0 \\ 0 & 0 & -3 \end{bmatrix},\quad \begin{bmatrix} -2 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 2 \end{bmatrix},\quad \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 12 & 4 & -3 \end{bmatrix}.$$

5. 设A,B是两个$n\times n$矩阵，它们的元素都在一个域k中。又设有另一域$K\supset k$，而A与B对域K相似(即存在$P\in \mathrm{GL}(n,K)$，使得$PAP^{-1}=B$)。证明A与B对域k也是相似的。

6. 证明矩阵A相似于它的转置A^T。

7. 设有矩阵A,B,C,D，使得分块矩阵

$$\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} 与 \begin{bmatrix} C & 0 \\ 0 & D \end{bmatrix}$$

相似(A与C的阶相等，B与D的阶相等)。证明A与C相似，B与D相似。

8. 如果一个实对称矩阵A是幂幺的，则$A^2=I$（I为幺矩阵)。

9. 如果一个线性变换σ满足$\sigma^n=0$(n为正整数)，则称σ是幂零的(nilpotent)。证明一个幂零的线性变换σ可以对角化(即其矩阵与一个对角矩阵相似)$\Longleftrightarrow \sigma=0$。

10. 找出一个实矩阵A，使$A^3=I$但$A^2\neq I$。

11. 设A,B是复向量空间的线性变换，满足$AB=BA$。证明A和B有公共的特征向量。

12. 设A是线性变换。证明$f(A)$以$f(\lambda)$为特征值，这里λ是A的特征值，$f(x)$是一元多项式。

13. 设A是可逆线性变换。证明A^{-1}以$1/\lambda$为特征值，这里λ是A的特征值。

§6 内积及正交坐标

在§3中，我们讨论了K向量空间$\mathrm{Hom}_K(V,W)$(参考定理4.5及定理4.6).其中有两个特别有意义的情形：一是$V=W$($\dim V<\infty$)的情形，在§4中，我们证明了若当标准式定理；二是$W=K$的情形，这是本节将要研究的对象。

定义4.17 $\mathrm{Hom}_K(V,K)$的元素称为V的**线性函数**，$\mathrm{Hom}_K(V,K)$称为V的**对偶空间**。

据据定理4.6，我们知道

$$\dim V<\infty \implies \dim \mathrm{Hom}_K(V,K)=\dim V,$$

于是V与$\mathrm{Hom}_K(V,K)$是同构的(读者注意，这是在$\dim V<\infty$的限制下)。

当$K=\mathbf{R}$或$\mathbf{C}$时，我们将引入“内积”的概念，并且用内积来实现V与$\mathrm{Hom}_K(V,K)$的同构。于是，我们有下列的定义。

定义4.18 设$K=\mathbf{R}$或$\mathbf{C}$。以$\bar{a}$表示a的复共轭数。一个二元函数

$$f:\ V\times V\to K,$$

$$f(v_1,v_2)=\langle v_1,v_2\rangle\in K,$$

如果适合下列条件，则称为V的**弱内积**：

1) $\langle\ ,\ \rangle$对第二个变数是线性的．即对任意固定的$v_1\in V$及对所有的$v_2,v_3\in V$，$a_2,a_3\in K$，恒有

$$\langle v_1, a_2v_2+a_3v_3\rangle = a_2\langle v_1,v_2\rangle + a_3\langle v_1,v_3\rangle;$$

2) $\langle v_1,v_2\rangle = \overline{\langle v_2,v_1\rangle}$;

3) $\langle\ ,\ \rangle$是非退化的，即

$$\langle v_1,v_2\rangle = 0,\qquad \forall v_2\in V \implies v_1 = 0.$$

如果$\langle\ ,\ \rangle$适合上述的条件 1)与 2)以及下列的较强的条件 3′)，则称为V的内积．

3′) $\langle v_1,v_1\rangle \geqslant 0$，$\forall v_1\in V$．$\langle v_1,v_1\rangle = 0 \Longrightarrow v_1 = 0$．

讨论 1) 条件 3′)显然较条件 3)为强，所以,内积自然是弱内积．不是内积的弱内积是存在的．下面的例16所举的物理学的“时-空”四维空间中，就有一个自然的弱内积．

2) 在$K=\boldsymbol{C}$时，弱内积与内积对第一个变数不是线性的．事实上，我们有

$$\begin{aligned}\langle a_1v_1+a_2v_2, v_3\rangle &= \overline{\langle v_3, a_1v_1+a_2v_2\rangle}\\ &= \overline{(a_1\langle v_3,v_1\rangle + a_2\langle v_3,v_2\rangle)} = \bar{a}_1\overline{\langle v_3,v_1\rangle} + \bar{a}_2\overline{\langle v_3,v_2\rangle}\\ &= \bar{a}_1\langle v_1,v_3\rangle + \bar{a}_2\langle v_2,v_3\rangle \neq a_1\langle v_1,v_3\rangle + a_2\langle v_2,v_3\rangle.\end{aligned}$$

当然,在特殊情况下,最后一个不等式也可能是等式．如果$K=\boldsymbol{R}$，则$\langle\ ,\ \rangle$对第一个变数是线性的．

例15 设$V=\boldsymbol{R}^3$．任取$v_1,v_2\in\boldsymbol{R}^3$，

$$v_1=\begin{bmatrix}a_1\\a_2\\a_3\end{bmatrix},\qquad v_2=\begin{bmatrix}b_1\\b_2\\b_3\end{bmatrix},$$

定义内积$\langle v_1,v_2\rangle$如下：

$$\begin{aligned}\langle v_1,v_2\rangle &= a_1b_1+a_2b_2+a_3b_3\\ &= \begin{bmatrix}a_1 & a_2 & a_3\end{bmatrix}\begin{bmatrix}b_1\\b_2\\b_3\end{bmatrix} = \begin{bmatrix}a_1\\a_2\\a_3\end{bmatrix}^T\begin{bmatrix}b_1\\b_2\\b_3\end{bmatrix} = v_1^Tv_2,\end{aligned}$$

不难看出此确为一内积。

应用这个内积，我们很容易把一些几何概念加以代数化。例如：

1）向量 v_1 的长度 $=\sqrt{a_1^2+a_2^2+a_3^2}=\sqrt{\langle v_1,v_1\rangle}$；

2）两向量 v_1,v_2 的距离

$$d=\sqrt{\sum_{i=1}^{3}(a_i-b_i)^2}=\sqrt{\langle v_1-v_2,v_1-v_2\rangle};$$

3）两向量 v_1,v_2 的夹角

$$\theta=\cos^{-1}\frac{\langle v_1,v_2\rangle}{\sqrt{\langle v_1,v_1\rangle\langle v_2,v_2\rangle}};$$

4）两向量 v_1,v_2 互相垂直的条件是 $\langle v_1,v_2\rangle=0$；

5）通过原点的平面的方程式：设以此平面上的点为端点的向量为 v，平面的法向量为 v_1，则平面的方程式为 $\langle v_1,v\rangle=0$；

6）通过向量 v_2 的端点的平面的方程式：设 v 及 v_1 如5)所示，则平面的方程式为 $\langle v_1,v-v_2\rangle=0$，即 $\langle v_1,v\rangle-\langle v_1,v_2\rangle=0$；

7）以原点为心，以 r 为半径的球面的方程式：设 v 为以球面上的点为端点的向量，则方程式为 $\langle v,v\rangle=r^2$。

例16　设 $V=\boldsymbol{R}^4$。我们定义一个类似于例15的内积。这是很容易的，读者不妨试试看。我们现在把 $\boldsymbol{R}^4$ 当成物理学中的“时-空”四维空间，考虑一个弱内积 $\langle\ ,\ \rangle$。令

$$v_1=\begin{bmatrix}a_1\\a_2\\a_3\\a_4\end{bmatrix},\qquad v_2=\begin{bmatrix}b_1\\b_2\\b_3\\b_4\end{bmatrix}.$$

定义 $\langle v_1,v_2\rangle$ 为

$$\langle v_1,v_2\rangle=a_1b_1+a_2b_2+a_3b_3-c^2a_4b_4,$$

上式的 c 表示光速。此时如果 $v_1\neq0$，可能有 $\langle v_1,v_1\rangle=0$。前三维是空间的三维，最后一维是时间。我们试解 $\langle v_1,v_1\rangle=0$ 这个方程式：

$$a_1^2 + a_2^2 + a_3^2 - c^2 a_4^2 = 0,$$

即

$$\pm\sqrt{a_1^2 + a_2^2 + a_3^2} = c a_4.$$

R^4 的原点(0,0,0,0)是空间及时间的原点。上式的解是空间的点(a_1, a_2, a_3)及时间 a_4，其中时间 a_4 恰好是光线从原点射到(a_1, a_2, a_3)的时间(正値)，或光线从(a_1, a_2, a_3)射到原点的时间(负値)。上式解的集合是“光锥”。我们可以作一图(图4.2)。

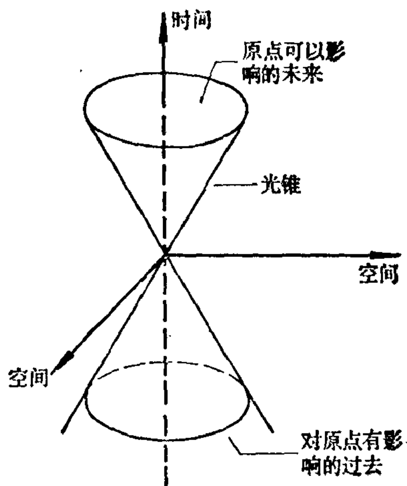


图 4.2

为了作图方便，仅把空间画成二维的。

例17 设 $V = \boldsymbol{C}^n$ 或 $\boldsymbol{R}^n$。任取 $v_1, v_2 \in V$,

$$v_1 = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}, \quad v_2 = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}.$$

定义“一般的”内积$\langle v_1, v_2 \rangle$如下：

$$\langle v_1, v_2 \rangle = \bar{v}_1^{\mathrm{T}} v_2 = \sum_{j=1}^{n} \bar{a}_j b_j.$$

上式的“-”表示复数的共轭。参考例15的1)—7)。当 $V = \boldsymbol{C}^n$ 时，除了3)的夹角 θ(此时 $\cos\theta$ 可能是复数，以致于 θ 沒有几何意义)外，其余的我们全可以应用到 $\boldsymbol{C}^n$ 里。简言之，我们可以把 1),2),4),5),6),7)当成几何概念的定义来建构复空间的几何学。

定理4.35 设 V 是 K 向量空间，K 是域 $\boldsymbol{R}$ 或域 $\boldsymbol{C}$。$\langle\ ,\ \rangle$ 是

V的弱内积。则

$$\{\langle v_1, \ \rangle: \ v_1 \in V\}$$

是$\mathrm{Hom}_K(V,K)$的子空间。如果$\dim V < \infty$，则两者相等。

证明 显然，$\langle v_1, \ \rangle$皆是V的线性函数(参考定义4.18的条件1))。又有

$$\sum a_j \langle v_j, \ \rangle = \sum a_j \overline{\langle \ ,v_j \rangle} = \sum \overline{(\bar{a}_j \langle \ ,v_j \rangle)}$$

$$= \overline{\left\langle \ ,\sum \bar{a}_j v_j \right\rangle} = \left\langle \sum \bar{a}_j v_j, \ \right\rangle,$$

故$\{\langle v_1, \ \rangle: \ v_1 \in V\}$是$\mathrm{Hom}_K(V,K)$的子空间。

如果$\dim V < \infty$，令$\{u_1, u_2, \cdots, u_n\}$为$V$的一组基。我们要证明$\{\langle u_1, \ \rangle, \langle u_2, \ \rangle, \cdots, \langle u_n, \ \rangle\}$是线性无关的。如此，便得出

$$\{\langle v_1, \ \rangle: \ v_1 \in V\} = \mathrm{Hom}_K(V,K)。$$

设有线性关系式$\sum_j a_j \langle u_j, \ \rangle = 0$，即$\left\langle \sum_j \bar{a}_j u_j, \ \right\rangle = 0$。由定义4.18的条件3)，即知

$$\sum_j \bar{a}_j u_j = 0。$$

而$\{u_j\}$是V的一组基，故$\bar{a}_j = 0 (j = 1, 2, \cdots, n)$。于是$a_j = 0$。这就证出了$\{\langle u_1, \ \rangle, \langle u_2, \ \rangle, \cdots, \langle u_n, \ \rangle\}$是线性无关的。 ▌

设V是有限维K向量空间，这里$K = \mathbf{R}$或$\mathbf{C}$。任取一组基$\{v_1, v_2, \cdots, v_n\}$，令$\rho_v: V \to K^n$为$V$的坐标系。设$\langle \ , \ \rangle$为一给定的弱内积。令$A \in \mathrm{Hom}_K(K^n, K^n)$为如下定义的矩阵：

$$a_{ij} = \langle v_i, v_j \rangle, \qquad A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}.$$

任取$u = b_1 v_1 + b_2 v_2 + \cdots + b_n v_n$，$w = c_1 v_1 + c_2 v_2 + \cdots + c_n v_n$。则有

(∗) $$\langle u,w\rangle=\sum_{i,j}\bar{b}_i c_j\langle v_i,v_j\rangle$$

$$=\overline{[b_1\ \ b_2\ \ \cdots\ \ b_n]}\,A\begin{bmatrix}c_1\\c_2\\\vdots\\c_n\end{bmatrix}.$$

如果我们在 K^n 中定义内积为

$$\left\langle\begin{bmatrix}b_1\\b_2\\\vdots\\b_n\end{bmatrix},\begin{bmatrix}c_1\\c_2\\\vdots\\c_n\end{bmatrix}\right\rangle=\overline{[b_1\ \ b_2\ \ \cdots\ \ b_n]}A\begin{bmatrix}c_1\\c_2\\\vdots\\c_n\end{bmatrix},$$

则(∗)式可写为

$$\langle u,w\rangle=\langle\rho_v(u),\rho_v(w)\rangle.$$

在这种意义下，A 即是 V 的弱内积$\langle\ ,\ \rangle$相对于基$\{v_1,v_2,\cdots,v_n\}$**的矩阵表示式。**

在选取基$\{v_1,v_2,\cdots,v_n\}$时，有一种特别优越的基，即所谓"正交基"，其定义如下：

定义4.19 一组基$\{v_1,v_2,\cdots,v_n\}$如适合下列条件，则称为(对弱内积$\langle\ ,\ \rangle$的)**正交基**：

$$\langle v_i,v_j\rangle=\pm\delta_{ij},$$

此处
$$\delta_{ij}=\begin{cases}1, & i=j,\\0, & i\neq j.\end{cases}$$

讨论 如果基$\{v_1,v_2,\cdots,v_n\}$是正交基，则弱内积的矩阵表示式是

$$A=\begin{bmatrix}\pm1 & & & 0\\ & \pm1 & & \\ & & \ddots & \\ 0 & & & \pm1\end{bmatrix}.$$

其对角线上$+1$的个数减去-1的个数，称为A的**符号差或弱内积**

$\langle\ ,\ \rangle$的符号差。不难看出，一个弱内积是内积当且仅当其符号差是 $n=\dim V$。

定理4.36 设$\langle\ ,\ \rangle$是有限维向量空间V的弱内积，则V有正交基。

证明 从 $V=V$ 开始，我们逐渐将V分解为

$$V=V_1\times V_2\times\cdots\times V_l,$$

使$\langle\ ,\ \rangle$作用在每个 V_i 上仍是弱内积，以及对任意的 $v_i\in V_i$, $v_j\in V_j$，如果 $i\neq j$，则恒有$\langle v_i,v_j\rangle=0$。最后我们要做到 $l=n$，$\dim V_i=1$，即实现V的完全分解。

从 $V=V$ 开始，假设我们已做到了 $V=V_1\times V_2\times\cdots\times V_l$ 的阶段。设 $\dim V_1>1$，我们要进一步分解V_1。任取V_1的一组基$\{u_1,u_2,\cdots,u_m\}$，则有两种可能：

1) $\langle u_j,u_j\rangle=0$, $\forall j=1,2,\cdots,m$;

2) 存在某个 j，使$\langle u_j,u_j\rangle\neq0$。不妨设 $j=1$。

在第 1)种情形下，我们要另取一组基$\{w_1,w_2,\cdots,w_m\}$，使之成为第 2)种情形。显然，$\langle u_1,u_j\rangle$不可能全为零，否则$\langle u_1,v_1\rangle=0,\forall v_1\in V_1$.这与$\langle\ ,\ \rangle$是$V_1$的弱内积的假设不符(请注意$\langle\ ,\ \rangle$是非退化的)。不妨设$\langle u_1,u_2\rangle\neq0$。如果 $\langle u_1,u_2\rangle$ 不是纯虚数，则取

$$w_1=u_1+u_2,\quad w_2=u_1-u_2,\quad w_3=u_3,\quad \cdots,\quad w_m=u_m,$$

就有

$$\begin{aligned}\langle w_1,w_1\rangle&=\langle u_1,u_1\rangle+\langle u_2,u_1\rangle+\langle u_1,u_2\rangle+\langle u_2,u_2\rangle\\&=\overline{\langle u_1,u_2\rangle}+\langle u_1,u_2\rangle\neq0.\end{aligned}$$

如果$\langle u_1,u_2\rangle$是纯虚数，则取

$$w_1=u_1+\mathrm{i}u_2,\quad w_2=u_1-\mathrm{i}u_2,\quad w_3=u_3,\quad \cdots,\quad w_m=u_m,$$

就有

$$\begin{aligned}\langle w_1,w_1\rangle&=\langle \mathrm{i}u_2,u_1\rangle+\langle u_1,\mathrm{i}u_2\rangle\\&=-\mathrm{i}\langle u_2,u_1\rangle+\mathrm{i}\langle u_1,u_2\rangle=2\mathrm{i}\langle u_1,u_2\rangle\neq0.\end{aligned}$$

综上所论，1)可以归结到2)的情形。

现设$\langle u_1,u_1\rangle \neq 0$。取另一组基$\{w_1,w_2,\cdots,w_m\}$如下：

$$w_1=u_1,$$

$$w_j=u_j-(\langle u_1,u_j\rangle/\langle u_1,u_1\rangle)u_1, \qquad j=2,\cdots,m.$$

请注意，从几何上看，$(\langle u_1,u_j\rangle/\langle u_1,u_1\rangle)u_1$即是$u_j$到$u_1$所确定的直线上的投影。不难检验

$$\langle w_1,w_j\rangle=\langle u_1,u_j\rangle-(\langle u_1,u_j\rangle/\langle u_1,u_1\rangle)\langle u_1,u_1\rangle=0.$$

取W_1为由$\{w_1\}$生成的向量空间，W_2为由$\{w_2,\cdots,w_m\}$生成的向量空间，则有

$$V_1=W_1\times W_2, \qquad V=W_1\times W_2\times V_2\times\cdots\times V_l.$$

容易看出，如果v,u属于$W_1,W_2,V_2,\cdots,V_l$中的不同者，则$\langle v,u\rangle=0$。我们尚须证明$\langle\ ,\ \rangle$作用在W_1,W_2上，仍是弱内积。事实上，我们仅须证明$\langle\ ,\ \rangle$在W_1,W_2上是非退化的。

在W_1上，如果$a\neq 0$，则

$$\langle aw_1,aw_1\rangle=a\bar{a}\langle w_1,w_1\rangle\neq 0,$$

所以$\langle\ ,\ \rangle$不是退化的。在W_2上，任取$u\in W_2$，如果$\langle u,w_2'\rangle=0$，$\forall w_2'\in W_2$，则任取$v\in V$，设

$$v=w_1'+w_2'+u_2'+\cdots+u_m',$$

此处$w_1'\in W_1$，$w_2'\in W_2$，$u_2'\in V_2$，$\cdots$，$u_m'\in V_m$，则有

$$\begin{aligned}\langle u,v\rangle&=\langle u,w_1'\rangle+\langle u,w_2'\rangle+\langle u,u_2'\rangle+\cdots+\langle u,u_m'\rangle\\&=0+0+0+\cdots+0=0.\end{aligned}$$

根据弱内积定义中的条件3)，我们立得$u=0$。所以$\langle\ ,\ \rangle$在W_2上也是非退化的。

以上证明了，如果$\dim V_1>1$，则V_1可以按照我们已定的条件进一步分解。自然，如果$\dim V_j>1$，也可如法分解。如此逐步进行，一直到完成分解，便有$\dim V_j=1$，$V=V_1\times V_2\times\cdots\times V_n$。此时，任取$V_j$的基$\{v_j'\}$，则必有$\langle v_j',v_j'\rangle\neq 0$，否则$\langle\ ,\ \rangle$在$V_j$上是退化的，不成为弱内积了。根据弱内积的条件2)，$\langle v_j',v_j'\rangle=\overline{\langle v_j',v_j'\rangle}$，所以$\langle v_j',v_j'\rangle$是实数，令$\langle v_j',v_j'\rangle=\pm a_j^2(a_j$

$\in \boldsymbol{R}$)，取$w'_j = v'_j/a_j$，立得$\langle w'_i, w'_j\rangle = \pm\delta_{ij}$。于是$\{w'_1, w'_2, \cdots, w'_n\}$是$V$的正交基。▍

讨论 1）如果$\langle\ ,\ \rangle$是内积，则易于看出$\langle\ ,\ \rangle$作用在V的任意非零子空间U上也是U的内积。所以，按照本定理，任意非零子空间U也有正交基。

2）一般言之，弱内积$\langle\ ,\ \rangle$作用在子空间U上，可能是退化的。例如在例16中，"光锥"上通过原点的直线都是一维子空间，在此直线上，$\langle\ ,\ \rangle$恒为零，故$\langle\ ,\ \rangle$为退化的。在此子空间内，自然不可能有正交基了。▍

一般言之，域K(不一定是$\boldsymbol{R}$或$\boldsymbol{C}$)上的向量空间V的任一线性变换$T\in \mathrm{Hom}_K(V,V)$，对应着V的对偶空间$\mathrm{Hom}_K(V,K)$的一个线性变换T^*，其定义如下：

$$(T^*f)(v) = f(T(v)),\quad \forall f\in \mathrm{Hom}_K(V,K),\ v\in V.$$

T^*显然是$\mathrm{Hom}_K(V,K)$的线性变换，称之为T的**伴随变换**。设$K=\boldsymbol{R}$或$\boldsymbol{C}$，V有一弱内积$\langle\ ,\ \rangle$，$\dim V<\infty$。根据定理1.35，$\mathrm{Hom}_K(V,K)$即是$\{\langle v_1,\ \rangle: v_1\in V\}$，所以对于任一$f=\langle v_1,\ \rangle\in \mathrm{Hom}_K(V,K)$，$T^*f$必可写成$\langle u,\ \rangle$的形式。于是，$T$(它规定了$T^*$)决定了$V$到自身的映射(仍记为$T^*$)：$T^*(v_1)=u$。容易验证，这个$T^*$: $V\to V$是一个线性变换，仍称为T的**伴随变换**。在这样的记号下，我们有

$$T^*(\langle v_1,\ \rangle) = \langle T^*(v_1),\ \rangle.$$

注意到$\mathrm{Hom}_K(V,K)$上的变换T^*的定义，即知

$$T^*(\langle v_1, v_2\rangle) = \langle v_1, T(v_2)\rangle,\qquad \forall v_2\in V,$$

故有

$$\langle T^*(v_1), v_2\rangle = \langle v_1, T(v_2)\rangle,\qquad \forall v_1, v_2\in V.$$

例18 设$K=\boldsymbol{R}$，V是可数无限维K向量空间。设V的一组基为$\{v_1, v_2, \cdots, v_n, \cdots\}$。定义内积$\langle\ ,\ \rangle$为

$$\left\langle \sum_{\text{有限}} a_i v_i,\ \sum_{\text{有限}} b_i v_i \right\rangle = \sum_i a_i b_i.$$

定义V的线性变换T为

$$T(v_1)=v_1, \quad T(v_i)=v_1+v_i, \quad \forall i>1.$$

T的伴随变换T^*作用在V的对偶空间$\mathrm{Hom}_K(V,K)$上。试问

$$T^*\langle v_1, \ \rangle \in \{\langle v, \ \rangle: v\in V\}?$$

答案是否定的。事实上

$$\begin{aligned} T^*\langle v_1, v_i\rangle &= \langle v_1, T(v_i)\rangle = \langle v_1, v_1+v_i\rangle \\ &= \langle v_1, v_1\rangle = 1, \quad \forall i=2,\cdots,n,\cdots. \end{aligned}$$

显然，不可能有任何一个$v\in V$，使$\langle v, \ \rangle$有此性质。

从上面的计算中，立得

$$\{\langle v, \ \rangle: v\in V\}\subsetneqq \mathrm{Hom}_K(V,K). \ \blacksquare$$

设$K=\boldsymbol{R}$或$\boldsymbol{C}$，$\dim V=n<\infty$，$\langle \ , \ \rangle$是V的弱内积。我们可以把T^*具体地写出来。任取$\{v_1,v_2,\cdots,v_n\}$为V的一组基，ρ为V的坐标系。令$A=[a_{ij}]_{n\times n}$为弱内积的矩阵表示式，即

$$[a_{ij}]_{n\times n}=[\langle v_i, v_j\rangle]_{n\times n}.$$

设$T\in \mathrm{Hom}_K(V,V)$，其作用如下：

$$T(v_i)=\sum_{j=1}^n b_{ji}v_j.$$

令$B=[b_{ij}]_{n\times n}$，即B为T的矩阵表示式。任取

$$u=\sum_{i=1}^n c_i v_i, \quad w=\sum_{j=1}^n d_j v_j,$$

则有

$$\begin{aligned} \langle u, T(w)\rangle &= \overline{\rho(u)}^T AB\rho(w) \\ &= \rho(u)^T(ABA^{-1})A\rho(w) \\ &= \overline{\overline{(ABA^{-1})^T\rho(u)}}^T A\rho(w). \end{aligned}$$

而
$$\langle T^*(u), w\rangle = \overline{C\rho(u)}^T A\rho(w),$$

其中C为T^*的矩阵表示式。故有

$$C=\overline{(ABA^{-1})^T}=(\bar{A}^T)^{-1}\bar{B}^T(\bar{A}^T).$$

因为 $a_{ij}=\langle v_i,v_j\rangle=\overline{\langle v_j,v_i\rangle}=\bar{a}_{ji}$，故 $\bar{A}^T=A$。于是 T^*的矩阵表示式为 $A^{-1}\bar{B}^TA$。如果此弱内积< , >是内积，则可选取V的正交基$\{v_1,v_2,\cdots,v_n\}$，即有 $A=I$(I 表示幺矩阵)。如此，T^*的矩阵表示式即是 $\bar{B}^T=B^*$。

综上所述，我们给出如下的定义。

定义4.20 设 $K=\mathbf{R}$ 或 $\mathbf{C}$，$\dim V=n<\infty$，< , >是V的弱内积。设 $T\subset \mathrm{Hom}_K(V,V)$。如果 $T=T^*$，则称 T为**自伴变换**。任给矩阵 $B\in \mathrm{FL}(n,K)$，如果 $B=B^*$，则称B为**自伴矩阵**。如果< , >为内积，任取V的正交基，则自伴变换的矩阵表示式是自伴矩阵。如果 $K=\mathbf{R}$，则称自伴变换为**对称变换**，自伴矩阵即是**对称矩阵**。

定义4.21 设 $K=\mathbf{R}$ 或 $\mathbf{C}$，$\dim V=n<\infty$，< , >是V的弱内积，又设 $T\in\mathrm{Hom}_K(V,V)$。如果对于所有的 $u,w\in V$，恒有$\langle T(u),T(w)\rangle=\langle u,w\rangle$，则称 T为**等距变换**或**酉变换**。显然，T为等距变换的充要条件是：T^*T为恒等变换。

定义4.22 设A为复数 $n\times n$ 矩阵。如果$A^*A=I$，则称A为**酉矩阵**或**正交矩阵**。

定理4.37 设 $K=\mathbf{R}$ 或 $\mathbf{C}$，$\dim V=n<\infty$，< , >是V的内积，又设 $T\in\mathrm{Hom}_K(V,V)$为等距变换。则对任取的正交基，T的矩阵表示式B恒为酉矩阵。

证明 参见定义4.20前面的讨论，自明。❙

设A是酉矩阵，我们把A具体地写出来：

$$A=\begin{bmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\a_{21}&a_{22}&\cdots&a_{2n}\\\cdots&\cdots&\cdots&\cdots\\a_{n1}&a_{n2}&\cdots&a_{nn}\end{bmatrix}=[u_1\ u_2\ \cdots\ u_n],$$

其中

$$u_i=\begin{bmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{ni} \end{bmatrix}, \qquad i=1,2,\cdots,n.$$

条件 $A^*A=I$ 即是

$$u_i^* u_i=\delta_{ij}=\begin{cases} 0, & i\neq j, \\ 1, & i=j. \end{cases}$$

也即向量集合$\{u_1,u_2,\cdots,u_n\}$是K^n对一般的内积(参考例14及例16)的一组正交基。所以酉矩阵也称为正交矩阵。

例19 在定义4.20及定义4.21中，如果$\langle\ ,\ \rangle$是内积，并且在K^n中取一般的内积，则有很自然的对应关系：

$$V\text{的正交基}\longleftrightarrow K^n\text{的标准坐标系},$$

在正交基下，有

$$\text{自伴变换}\longleftrightarrow\text{自伴矩阵},$$
$$\text{等距变换}\longleftrightarrow\text{酉矩阵}.$$

如果$\langle\ ,\ \rangle$仅为弱内积，则以上的对应关系皆不成立。例如：令

$V=\mathbf{R}^2$，弱内积$\langle\ ,\ \rangle$为(参考例15)

$$\left\langle\begin{bmatrix} a_1 \\ a_2 \end{bmatrix},\begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\right\rangle=a_1b_1-a_2b_2.$$

设T为下式所定义的线性变换：

$$T\left(\begin{bmatrix} a_1 \\ a_2 \end{bmatrix}\right)=\begin{bmatrix} \frac{1}{2}(3a_1-a_2) \\ \frac{1}{2}(a_1+a_2) \end{bmatrix},$$

则有

$$\left\langle\begin{bmatrix} a_1 \\ a_2 \end{bmatrix},T\left(\begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\right)\right\rangle=\frac{1}{2}a_1(3b_1-b_2)-\frac{1}{2}a_2(b_1+b_2)$$

$$=\frac{1}{2}(3a_1-a_2)b_1-\frac{1}{2}b_2(a_1+a_2)$$

$$=\left\langle\begin{bmatrix}(3a_1-a_2)/2\\(a_1+a_2)/2\end{bmatrix},\begin{bmatrix}b_1\\b_2\end{bmatrix}\right\rangle$$

$$=\left\langle T\left(\begin{bmatrix}a_1\\a_2\end{bmatrix}\right),\begin{bmatrix}b_1\\b_2\end{bmatrix}\right\rangle.$$

所以立得$T=T^*$，即T为自伴变换。取正交基

$$\left\{\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}\right\},$$

则T的矩阵表示式B及弱内积$\langle\ ,\ \rangle$的矩阵表示A分别为

$$B=\begin{bmatrix}3/2&-1/2\\1/2&1/2\end{bmatrix},\qquad A=\begin{bmatrix}1&0\\0&-1\end{bmatrix}.$$

而T^*的矩阵表示式为

$$B=A^{-1}B^*A\neq B^*.$$

所以在弱内积时，自伴变换在正交基下的矩阵不一定是自伴矩阵。

习　题

1. 设f_1,f_2是三维空间V的两个线性函数。问常数a_1,a_2必须适合什么条件才能使$f(x)=a_1$和$f(x)=a_2$有公解？

2. 举例说明$\langle\ ,\ \rangle$是弱内积，不能保证$v\neq0$时

$$\langle v,v\rangle\neq0.$$

3. 设$\{\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n\}$及$\{\xi_1,\xi_2,\cdots,\xi_n\}$是向量空间$V$的两组基，$C$为过渡矩阵，即

$$(\xi_1,\xi_2,\cdots,\xi_n)=(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n)C.$$

设$\langle\ ,\ \rangle$是V的弱内积，在$\{\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n\}$和$\{\xi_1,\xi_2,\cdots,\xi_n\}$下的矩阵表示式分别为$A$和$B$。试用$C$和$A$表出$B$。

4. 证明弱内积的符号差与标准正交基的选择无关。

5. 设$\langle\ ,\ \rangle$是$\mathbf{C}$向量空间V的弱内积。证明$\mathcal{A}$是酉变换$\Longleftrightarrow$ $\mathcal{A}$在某组标准正交基下的矩阵A适合

$$A^TGA=G,$$

其中

$$G=\begin{bmatrix} 1 & & & & & 0 \\ & \ddots & & & & \\ & & 1 & & & \\ & & & -1 & & \\ & 0 & & & \ddots & \\ & & & & & -1 \end{bmatrix}.$$

6. 设< ，>是向量空间V的内积．定义一个向量v的范数(norm)为

$$\|v\|=\sqrt{\langle v,v\rangle}.$$

范数相当于长度．证明

$$\|v+u\|^2+\|v-u\|^2=2\|v\|^2+2\|u\|^2.$$

试用几何学解释上式．

7. 设< ，>是 $\boldsymbol{C}$ 向量空间V的内积，V_1是V的子空间．定义

$$V_1^{\perp}=\{x\in V:\ \langle v,x\rangle=0,\quad \forall v\in V_1\}.$$

称$V_1^{\perp}$为V_1的**正交补**．证明$V_1^{\perp}$是V的子空间，且

$$V=V_1\oplus V_1^{\perp}.$$

考虑当< ，>是V的弱内积时上述二结论是否成立？

8. 设< ，>是 $\boldsymbol{C}$ 向量空间V的内积，A和B是线性变换．证明

(1) $(\lambda A)^*=\bar{\lambda}A^*$，其中$\lambda\in\boldsymbol{C}$；

(2) $(A+B)^*=A^*+B^*$；

(3) $(AB)^*=B^*A^*$.

9. 对于a的哪些值，下面的矩阵是酉矩阵？

(1) $\begin{bmatrix} a & 0 \\ 1 & 1 \end{bmatrix}$，　　(2) $\begin{bmatrix} a & 1/2 \\ -1/2 & a \end{bmatrix}$.

10. 设< ，>是 $\boldsymbol{C}$ 向量空间V的内积，A是自伴变换．证明对于任意的$v\in V$，$\langle A(a),a\rangle$总是实数．

§7 谱 论

令A为一线性变换，则A的特征值的集合又称为A的谱的集合。在物理学的量子力学中，一个物理量——例如质量、能量、光的频率等等——常对应一个自伴变换A，而这个物理量的测度结果的纯态——例如光谱分析仪得出的光谱——即是这个自伴变换A的特征值。所以，特征值又称为谱。

在本节里，我们假定V为有限维的向量空间，而且有一内积。我们将要证明两个定理：

1) 设V为实数或复数向量空间，则对于V上任一自伴变换A，都存在着相应的正交基$\{v_1,v_2,\cdots,v_n\}$，使A的作用为实数对角矩阵的作用，即

$$A(v_i)=\lambda_i v_i, \qquad i=1,2,\cdots,n,$$

其中$\lambda_i\in\boldsymbol{R}$。

2) 设V为复数向量空间，则对V上任一等距变换(即酉变换)A，都存在着相应的正交基$\{v_1,v_2,\cdots,v_n\}$，使A的作用为对角矩阵的作用，即

$$A(v_i)=\lambda_i v_i, \qquad i=1,2,\cdots,n,$$

其中$\lambda_i\in\boldsymbol{C}$，且$\lambda_i$的绝对值为1。

上述的第二个定理对实数向量空间幷不成立。可参看例21。

我们先证明四个引理。

引理1 设V是有限维的复数向量空间，$\langle\ ,\ \rangle$是V的內积，A是V的自伴变换，则A的特征值皆是实数。

证明 设λ是A的特征值，v是特征值λ的特征向量。请注意，λ可为零，但v不能为零向量。按照自伴变换的定义，有

$$\begin{aligned}\lambda\langle v,v\rangle&=\langle v,A(v)\rangle=\langle A(v),v\rangle\\&=\langle\lambda v,v\rangle=\bar{\lambda}\langle v,v\rangle,\end{aligned}$$

于是
$$(\lambda-\bar{\lambda})\langle v,v\rangle=0, \qquad \lambda=\bar{\lambda},$$

即λ为实数。▎

引理2 设V是有限维的实数向量空间，< , >是V的内积，A是V的自伴变换。则A的特征多项式(即A的不变因子$c_1(x)$，$c_2(x),\cdots,c_l(x)$的乘积)可分解成实数一次多项式的乘积。

证明 任取V的一组正交基$\{v_1,v_2,\cdots,v_n\}$。令A对$\{v_1,v_2,\cdots,v_n\}$的矩阵表示式为$B\in \mathrm{Hom}_R(\boldsymbol{R}^n,\boldsymbol{R}^n)$。按照定义4.15及定理4.30，我们要证$B$的特征多项式可以完全分解成实数一次多项式的乘积。

我们考虑$B\in \mathrm{Hom}_R(\boldsymbol{R}^n,\boldsymbol{R}^n)\subset \mathrm{Hom}_C(\boldsymbol{C}^n,\boldsymbol{C}^n)$。因为$B$为自伴矩阵，自然有$B^*=\overline{B}^T=B$。于是，不论在$\mathrm{Hom}_R(\boldsymbol{R}^n,\boldsymbol{R}^n)$中考虑，还是在$\mathrm{Hom}_C(\boldsymbol{C}^n,\boldsymbol{C}^n)$中考虑，$B$总是自伴矩阵。令$B$的特征多项式为

$$f(x)=\det(xI-B).$$

在$\boldsymbol{C}[x]$中$f(x)$可分解成一次多项式的乘积

$$f(x)=\prod_{i=1}^{n}(x-d_i),$$

此处d_i为B作用在$\boldsymbol{C}^n$上的特征值。根据上一引理，d_i皆为实数，于是B作用在$\boldsymbol{R}^n$上的特征多项式(同是$f(x)=\det(xI-B)$)可以分解成实数一次多项式的乘积。▎

根据引理1及引理2，应用定理4.25的结果，不论$K=\boldsymbol{R}$或$\boldsymbol{C}$，对应于K向量空间V上的自伴变换A，皆存在V的一组基，使A的矩阵表示式为若当标准式

$$\begin{bmatrix} J_1 & & & 0 \\ & J_2 & & \\ & & \ddots & \\ 0 & & & J_m \end{bmatrix},$$

其中的块矩阵J_i皆形如

$$
\begin{bmatrix} c_j & & & 0 \\ 1 & c_j & & \\ & \ddots & \ddots & \\ 0 & & 1 & c_j \end{bmatrix},
$$

其中c_j为实数。我们要证明A的矩阵表示式为对角矩阵，也即所有的块矩阵J_j皆是1×1的矩阵。不妨设$J_j=J_1$(同法可证其余的)。设J_1是$l\times l$的矩阵。假若$l>1$，则有

$$
A(w_s)=c_1w_s+w_{s+1}, \qquad \forall\, s<l,
$$

$$
A(w_l)=c_1w_l,
$$

其中$w_1,\cdots,w_l$为使得A的矩阵表示式呈若当标准式的前l个基向量。计算下式：

$$
\langle w_{l-1},A(w_l)\rangle=\langle w_{l-1},c_1w_l\rangle=c_1\langle w_{l-1},w_l\rangle,
$$

由于A是自伴变换，所以上式左端又等于

$$
\begin{aligned}
\langle A(w_{l-1}),w_l\rangle &= \langle c_1w_{l-1}+w_l,w_l\rangle \\
&= \bar{c}_1\langle w_{l-1},w_l\rangle+\langle w_l,w_l\rangle \\
&= c_1\langle w_{l-1},w_l\rangle+\langle w_l,w_l\rangle
\end{aligned}
$$

(此式计算中应用了$c_1\in \boldsymbol{R}$的事实)，于是得出$\langle w_l,w_l\rangle=0$。这与内积的定义相违。总上所论，我们有下面的引理：

引理3 条件如引理1或者引理2。则存在V的基，使A的矩阵表示式为对角矩阵。❙

对于自伴变换A的不同的特征值$\lambda_1\neq\lambda_2$，其特征子空间V_{λ_1}及V_{λ_2}有下述关系：

引理4 条件如引理1或者引理2。设有A的不同的特征值$\lambda_1\neq\lambda_2$，及其特征子空间V_{λ_1}及V_{λ_2}。则对于任意的$v_1\in V_{\lambda_1}$，$v_2\in V_{\lambda_2}$，恒有$\langle v_1,v_2\rangle=0$。

证明 由于$\lambda_1,\lambda_2\in \boldsymbol{R}$，故有

$$
\begin{aligned}
\lambda_1\langle v_1,v_2\rangle &= \langle \lambda_1v_1,v_2\rangle=\langle A(v_1),v_2\rangle=\langle v_1,A(v_2)\rangle \\
&= \langle v_1,\lambda_2v_2\rangle=\lambda_2\langle v_1,v_2\rangle,
\end{aligned}
$$

所以 $$(\lambda_1-\lambda_2)\langle v_1,v_2\rangle=0,$$

即有 $$\langle v_1,v_2\rangle=0. \blacksquare$$

给定自伴变换A，选取V的一组基$\{w_1,w_2,\cdots,w_n\}$，使A的矩阵表示式为对角矩阵。然后按照A的特征值$\{\lambda_1,\lambda_2,\cdots,\lambda_m\}$重新排列基向量，使前几个生成$V_{\lambda_1}$，其余几个生成$V_{\lambda_2}$，等等。因为內积$\langle\ ,\ \rangle$在每个$V_{\lambda_j}$上的作用就是$V_{\lambda_j}$的一个內积，根据定理4.36，可以在每个$V_{\lambda_j}$里选取一组正交基。令这些正交基的并集为$\{u_1,u_2,\cdots,u_n\}$，则根据引理4，立得$\{u_1,u_2,\cdots,u_n\}$是$V$的正交基。自然的，$A$对$\{u_1,u_2,\cdots,u_n\}$的矩阵表示式是对角矩阵。于是我们有：

定理4.38 设V是有限维的K向量空间，$K=\mathbf{R}$或$\mathbf{C}$，$\langle\ ,\ \rangle$是V的內积，A是V的自伴变换。则存在V的正交基$\{u_1,u_2,\cdots,u_n\}$及实数$\lambda_1,\lambda_2,\cdots,\lambda_n$，使

$$A(u_i)=\lambda_i u_i,\qquad i=1,2,\cdots,n,$$

也即A对$\{u_1,u_2,\cdots,u_n\}$的矩阵表示式是实数对角矩阵。

证明 见上面的讨论。■

例20 任取一个实系数的n元二次多项式如下：

$$f(x_1,x_2,\cdots,x_n)=\sum_{i\geq j}a_{ij}x_ix_j+\sum_i b_ix_i+c.$$

令d_{ij}定义如下：

$$d_{ii}=a_{ii},\qquad \forall i;$$

$$d_{ij}=d_{ji}=\frac{1}{2}a_{ij},\qquad i>j.$$

令矩阵D为

$$D=\begin{bmatrix} d_{11} & d_{12} & \cdots & d_{1n}\\ d_{21} & d_{22} & \cdots & d_{2n}\\ \cdots & \cdots & \cdots & \cdots\\ d_{n1} & d_{n2} & \cdots & d_{nn}\end{bmatrix},$$

则$D^T=D$。不难看出

$$f(x_1,x_2,\cdots,x_n)=\begin{bmatrix}x_1\\x_2\\\vdots\\x_n\end{bmatrix}^T D\begin{bmatrix}x_1\\x_2\\\vdots\\x_n\end{bmatrix}+\sum_{i=1}^n b_ix_i+c.$$

在R^n内采用一般的内积：$\langle v,u\rangle=v^T\cdot u$，则$D$自然定义一自伴变换，即

$$v^T\cdot(Du)=(D^Tv)^T\cdot u=(Dv)^T\cdot u.$$

根据定理4.38，存在一正交矩阵C及一对角矩阵E，使

$$D=C^{-1}EC.$$

因为正交矩阵C适合关系式$C^*C=I$，在目前这个实数的例子中，

$$C^*=\overline{C}^T=C^T,$$

故$C^TC=I$。于是$C^{-1}=C^T$。所以上式可以写成

$$D=C^TEC.$$

代入原式，立得

$$f(x_1,\cdots,x_n)=\begin{bmatrix}x_1\\\vdots\\x_n\end{bmatrix}^T C^TEC\begin{bmatrix}x_1\\\vdots\\x_n\end{bmatrix}+\sum_{i=1}^n b_ix_i+c$$

$$=\left(C\begin{bmatrix}x_1\\\vdots\\x_n\end{bmatrix}\right)^T E\left(C\begin{bmatrix}x_1\\\vdots\\x_n\end{bmatrix}\right)+\begin{bmatrix}b_1\\\vdots\\b_n\end{bmatrix}^T C^TC\begin{bmatrix}x_1\\\vdots\\x_n\end{bmatrix}+c.$$

令

$$\begin{bmatrix}y_1\\\vdots\\y_n\end{bmatrix}=C\begin{bmatrix}x_1\\\vdots\\x_n\end{bmatrix},\quad\begin{bmatrix}b'_1\\\vdots\\b'_n\end{bmatrix}=C\begin{bmatrix}b_1\\\vdots\\b_n\end{bmatrix},$$

则二次多项式f可写成

$$f=\sum_{i=1}^n\lambda_iy_i^2+\sum_{i=1}^n b'_iy_i+c,$$

此处λ_i为对角矩阵E的对角线上的实数，即D的特征值。

以上的讨论，对二次曲面的分类很有用处。在两个变数的时候，二次曲面即二次曲线，

$$f(x_1,x_2)=a_{11}x_1^2+a_{12}x_1x_2+a_{22}x_2^2+b_1x_1+b_2x_2+c.$$

应用上面的讨论，f 又可写成

$$f=\begin{bmatrix} y_1 & y_2 \end{bmatrix}\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}\begin{bmatrix} y_1 \\ y_2 \end{bmatrix}+\begin{bmatrix} b'_1 & b'_2 \end{bmatrix}\begin{bmatrix} y_1 \\ y_2 \end{bmatrix}+c$$

$$=\lambda_1y_1^2+\lambda_2y_2^2+b'_1y_1+b'_2y_2+c.$$

此处$\{y_1,y_2\}$也是正交坐标系。按照λ_1,λ_2的值，二次曲线可分类为：1）椭圆：$\lambda_1\lambda_2>0$；2）双曲线：$\lambda_1\lambda_2<0$；3）抛物线：$\lambda_1\lambda_2=0$。同法我们也可以将三维空间的二次曲面进行分类。▌

以下我们处理等距变换(即酉变换)的“谱论”。

引理5 设V是有限维的复数向量空间，$\langle\ ,\ \rangle$是内积，A是V的等距变换。则A的特征值的绝对值皆是1。

证明 设λ是A的特征值，v是特征值λ的特征向量。按照等距变换的定义，则有

$$\langle v,v\rangle=\langle A(v),A(v)\rangle=\langle\lambda v,\lambda v\rangle=\bar{\lambda}\lambda\langle v,v\rangle,$$

故

$$|\lambda|^2=\bar{\lambda}\lambda=1,\qquad |\lambda|=1. ▌$$

我们现在证明A的若当标准式为对角矩阵。就像在引理3以前的讨论一样，仅须证明所有的若当块矩阵都是1×1的矩阵。任取A的一个若当块矩阵J，假设

$$J=\begin{bmatrix} c & & & 0 \\ 1 & c & & \\ & \ddots & \ddots & \\ 0 & & 1 & c \end{bmatrix}_{l\times l},\quad l>1.$$

令$\{w_1,w_2,\cdots,w_l\}$为相应的一部分基向量，则有

$$A(w_s)=cw_s+w_{s+1},\qquad s<l,$$

$$A(w_l)=cw_l.$$

按照引理5，$|c|=1$。计算下式：

$$\langle w_{l-1}, w_l\rangle = \langle A(w_{l-1}), A(w_l)\rangle = \langle cw_{l-1}+w_l, cw_l\rangle$$
$$= \bar{c}c\langle w_{l-1}, w_l\rangle + c\langle w_l, w_l\rangle$$
$$= \langle w_{l-1}, w_l\rangle + c\langle w_l, w_l\rangle,$$

故$\langle w_l, w_l\rangle = 0$。这与内积的定义矛盾。于是我们证出

引理6 条件如引理5。则存在V的基，使A的矩阵表示式是对角矩阵。

类似于引理4，我们也有下面的引理。

引理7 条件如引理5。设有A的不同的特征值$\lambda_1 \neq \lambda_2$，及其相应的特征子空间 $V_{\lambda_1}, V_{\lambda_2}$。则对于任意的$v_1 \in V_{\lambda_1}$，$v_2 \in V_{\lambda_2}$，恒有$\langle v_1, v_2\rangle = 0$。

证明 $\langle v_1, v_2\rangle = \langle A(v_1), A(v_2)\rangle = \langle \lambda_1 v_1, \lambda_2 v_2\rangle = \bar{\lambda}_1\lambda_2\langle v_1, v_2\rangle$。由于$\lambda_1\bar{\lambda}_1 = 1$，故$\bar{\lambda}_1 = \lambda_1^{-1}$。代入上式，有

$$\langle v_1, v_2\rangle = \frac{\lambda_2}{\lambda_1}\langle v_1, v_2\rangle.$$

但是$\lambda_1 \neq \lambda_2$，故必有$\langle v_1, v_2\rangle = 0$。❙

综合上面所证的几个引理，我们立得：

定理4.39 设V是有限维的复数向量空间，$\langle\ ,\ \rangle$是内积，A是V的等距变换(即酉变换)。则存在V的正交基$\{u_1, u_2, \cdots, u_n\}$，及绝对值为1的复数$\lambda_1, \lambda_2, \cdots, \lambda_n$，使

$$A(u_i) = \lambda_i u_i \quad i = 1, 2, \cdots, n,$$

也即A对$\{u_1, u_2, \cdots, u_n\}$的矩阵表示式是特征值$\lambda_i$的绝对值皆等于1的对角矩阵。

例21 对于实数向量空间，定理4.39是不成立的。例如在实数平面上，取一转角不等于$n\times 180°$(n为整数)的旋转A。A自然是等距变换，但A显然移动每一条通过原点的直线，故A并无实数的特征值，自然A的矩阵表示式也不相似于对角矩阵。

习 题

以下设V是$\boldsymbol{C}$向量空间，< , >是内积。

1．如果线性变换A满足$AA^*=A^*A$，则称A是一个**正规变换**。证明

(1) 自伴变换和酉变换都是正规变换；

(2) 若A为正规变换，则A和A^*有共同的特征向量，且特征值互相共轭；

(3) 若A为正规变换，则属于A的不同特征值的特征向量互相正交。

2．设A是正定矩阵(即A是实对称矩阵(行数为n)，且对任意的

$$X=[\ x_1 \quad x_2 \quad \cdots \quad x_n\ ]^T\in \boldsymbol{R}^n,$$

都有$X^TAX\geqslant 0$，而仅当$X=0$时才有$X^TAX=0$)。证明A的特征值皆为正数。

3．设A是V的自伴变换。如果$\langle A(\alpha),\alpha\rangle>0$，$\forall\alpha\in V\backslash\{0\}$，则称$A$为正定的自伴变换。证明：

A是正定的自伴变换$\Longleftrightarrow A$的特征值皆为正数。

4．设A是V的可逆自伴变换，证明A^2是正定的自伴变换。

5．设A是V的可逆线性变换，证明AA^*是正定的自伴变换。

6．设A是V的自伴变换。又设λ是A的一个特征值，且是A的特征多项式的k重根。证明V的属于λ的特征子空间V_λ的维数等于k。

7．设T是V的正定自伴变换，A是T在一组标准正交基下的矩阵。对于$X=[\ x_1 \quad x_2 \quad \cdots \quad x_n\ ]^T\in\boldsymbol{C}^n$，定义

$$f(X)=\overline{X}^TAX.$$

证明存在可逆矩阵C，使得

$$f(X)=y_1^2+y_2^2+\cdots+y_n^2,$$

其中$X=C\cdot[\ y_1\quad y_2\quad \cdots\quad y_n\ ]^T$。

8. 设A是$n\times n$自伴矩阵。证明存在$n\times n$可逆矩阵G，使得

$$A=\bar{G}G^T.$$

9. 设A是V的线性变换，满足$A^*=-A$。证明A的特征值皆是零或纯虚数。特别地，实反对称矩阵的特征值皆是零或纯虚数。

第五章 一元多项式的解及域论

§1 C的代数封闭性

在一般科学或数学里，对于某些数量、数据以及函数，通常先求得它们必须适合的必要条件(这些必要条件常表现成一组方程式)，然后进一步运用推理的方法，导出这些数量、数据及函数来．第一个步骤(求得必要条件的步骤)分属于各种学科与数学的领域．第二个步骤(从必要条件求解)属于数学的范围．这是数学的精妙功夫，也是数学的饶有趣味的所在．

按照这些方程的类别，这些必要条件可以分成代数方程式、微分方程式、积分方程式等等．代数学的要义是处理代数方程组的解的集合，以及用代数的方法处理一些非代数性的方程组，并从此推论出一些数学的性质．

在前几章，我们已经遇到不少这一类的例子．例如：

1) 求一组同余式的公解，解的存在性及在某种意义下的唯一性(中国剩余定理，即定理1.10)；

2) 两个二元多项式的公解(第三章例8)；

3) 从一个矩阵$A\in \mathrm{Hom}_C(\boldsymbol{C}^n,\boldsymbol{C}^n)$的特征多项式$\det(xI-A)$求得$A$的若当标准式的有限的几种可能的形式．从而知道选择适当的坐标系以后，A的几种可能的作用(第四章§5)；

4) 从奇次实数多项式皆有实数解，利用特征多项式，推出$\boldsymbol{R}^{2n+1}$的旋转皆有旋转轴(第四章 例14)．

在3)与4)中，特征多项式$\det(xI-A)\in K[x]$ (K为$\boldsymbol{R}$或$\boldsymbol{C}$)．实际上，把K中的元素a与aI认同后，K成了$\mathrm{Hom}_K(K^n,K^n)$的子环．令$L=\mathrm{Hom}_K(K^n,K^n)$，则可以考虑$K[x]$中的元素$\det(xI-A)$

在L中的根。一般言之，设R为一交换环，S是包含R的一个环，$f(x)\in R[x]$，则在S中求$f(x)=0$的解是有意义的。

关于一组方程式的解，最简单的情形是求一个一元多项式在域K中的根。第三章中已有关于根的个数的命题（定理3.15的系2）。

在上面的3)中，一个特征多项式虽然只有有限个若当标准式的解，然而在$\mathrm{Hom}_C(\boldsymbol{C}^n,\boldsymbol{C}^n)$里却有无限多个解。这是因为$\mathrm{Hom}_C(\boldsymbol{C}^n,\boldsymbol{C}^n)$是环，而非域，所以不适合定理3.15的系2.

有一类重要的域是所谓"代数封闭域"，见下定义。

定义5.1 设K是域，如果任意非常数的多项式$f(x)\in K[x]$在K中皆最少有一根，则称K为**代数封闭域**。

定理5.1 以下的三个条件皆等同，因此条件2)与3)皆可作为代数封闭域的定义：

1) K是代数封闭域；

2) $K[x]$的不可分解的元素皆是一次多项式；

3) $K[x]$中的非常数的多项式皆可分解成一次多项式的乘积。

证明 1)$\Longrightarrow$2)．设$f(x)$为不可分解的元素，于是$f(x)$非零非可逆，即$f(x)\notin K$。所以$f(x)$是非常数的多项式。按照定义5.1，$f(x)$最少有一个根。令此根为a。由欧几里得算法，存在$d(x),r(x)\in K[x]$，使

$$f(x)=d(x)(x-a)+r(x),\quad \deg r(x)<\deg(x-a)=1.$$

于是$r(x)=r\in K$。将$x=a$代入上式，立得：$0=f(a)=r$，即有

$$f(x)=d(x)(x-a).$$

因为$f(x)$不可分解，所以必有$d(x)=d\in K$，于是$f(x)$是一次式。

2)$\Longrightarrow$3)．因为$K[x]$是唯一分解的整环，所以任意非常数的多项式皆可分解成不可分解的元素的乘积。于是从2)立得3)．

3)$\Longrightarrow$1)．任取一非常数的多项式$f(x)\in K[x]$，按照3)，

我们有

$$f(x)=\prod_i (a_i x-b_i),\quad a_i \neq 0.$$

于是$x=b_1/a_1\in K$显然是$f(x)$的根。 ▌

讨论 实数域$\boldsymbol{R}$显然不是代数封闭的。例如$x^2+1\in \boldsymbol{R}[x]$在$R$中就没有根，因为任取$a\in R$，则$a^2\geqslant 0$，于是$a^2+1>0$。 ▌

下面这个定理是所谓"代数基本定理"。

定理5.2(代数基本定理) 复数域$\boldsymbol{C}$是代数封闭域。

证明一 应用复变函数论的Liouville定理：在$\boldsymbol{C}$上有界的解析函数皆是常值函数。假设一非常数的多项式$f(x)\in \boldsymbol{C}[x]$恒不为零。令$g(x)=1/f(x)$。则$g(x)$为解析函数。取一适当大的圆盘

$$D_k=\{x:\ |x|<k\}.$$

因为

$$\lim_{|x|\to\infty}\frac{1}{f(x)}=0,$$

所以当k充分大时，有

$$|g(x)|=\frac{1}{|f(x)|}<1,\qquad \forall x\notin D_k.$$

而$g(x)$为连续函数，所以$g(x)$在D_k上为有界的，于是$g(x)$在$\boldsymbol{C}$上亦有界。按照Liouville定理，$g(x)$为一常值函数，也即$f(x)$为一常值函数。 ▌

证明二 应用复变函数论的"极小模原则"：一个非常数的解析函数在定义域内不可能取得非零的极小模。设多项式$f(x)\in \boldsymbol{C}[x]$恒不为零。取一适当大的圆盘$D_k=\{x:\ |x|\leqslant k\}$，使得

$$|f(x)|\geqslant |f(0)|,\qquad \forall x\notin D_k.$$

而$|f(x)|$是连续实函数，所以在圆盘D_k上必有极小值。于是此极小值必为$f(x)$在$\boldsymbol{C}$上的极小模。按照极小模原则，$f(x)$必为常数。 ▌

证明三 我们先对多项式证明极小模原则，再利用上面的证

明二．假设$f(x)$在$x=a$点取得非零的极小模。不妨即设$a=0$。令$f(0)=c\neq 0$。可以考虑$c^{-1}f(x)$，如此，不妨即设$f(0)=1$。令$f(x)$的展开式如下：

$$f(x)=1+a_n x^n+a_{n+1}x^{n+1}+\cdots+a_m x^m,$$

此处$a_n\neq 0$。上式又可以整理如下：

$$f(x)=1+a_n x^n(1+b_1 x+\cdots+b_{m-n}x^{m-n}).$$

令 $x=t/\sqrt[n]{-a_n}$，而令 t 为正实数趋于零。则有

$$f(t/\sqrt[n]{-a_n})=1-t^n(1+\varepsilon(t)),$$

其中$\lim\limits_{t\to+0}|\varepsilon(t)|=0$。于是，当$t$充分小时，有

$$\begin{aligned}|f(t/\sqrt[n]{-a_n})|&=|1-t^n-t^n\varepsilon(t)|\\&\leqslant|1-t^n|+t^n|\varepsilon(t)|<1,\end{aligned}$$

这与$f(0)=1$是极小模的假设矛盾。这就证明了对多项式的极小模原则。接下去应用证明二，便得到本定理。▎

根据代数基本定理，非常数的多项式$f(x)\in \mathbf{C}[x]$皆有复数根。于是，如果$f(x)\in\mathbf{Q}[x]$，则$f(x)$自然有复数根。我们有下面的定义。

定义5.2 非常数的多项式$f(x)\in\mathbf{Q}[x]$的复数根称为**代数数**。反之，如果一个复数c不是任何非常数的有理多项式的根，则称c为**超越数**。

我们要证明代数数的集合是可数的。首先我们证明下面的引理。

引理 $\mathbf{Q}[x]$是可数集。

证明 令$P_n=\{f(x):\ \deg f(x)\leqslant n\}$。不难看出$\{1,x,x^2,\cdots,x^n\}$是$P_n$作为$\mathbf{Q}$向量空间的一组基。于是有

$$\dim P_n=n+1,$$

立得P_n与$n+1$个$\mathbf{Q}$的直积$\mathbf{Q}\times\mathbf{Q}\times\cdots\times\mathbf{Q}$同构。而且

$$\underbrace{\mathbf{Q}\times\mathbf{Q}\times\cdots\times\mathbf{Q}}_{n+1\text{个}}=\bigcup_{a\in\mathbf{Q}}\{a\}\times\underbrace{\mathbf{Q}\times\mathbf{Q}\times\cdots\times\mathbf{Q}}_{n\text{个}},$$

按照数学归纳法，可以假设 n 个 $\boldsymbol{Q}$ 的直积是可数的，于是上式表明 $n+1$ 个 $\boldsymbol{Q}$ 的直积是可数个可数集的并集。按照定理 1.1 的系，我们得知 $n+1$ 个 $\boldsymbol{Q}$ 的直积也是可数的。于是，我们立得 P_n 是可数集。

进一步看，我们有

$$\boldsymbol{Q}[x]=\bigcup_{n=1}^{\infty}P_n,$$

故 $\boldsymbol{Q}[x]$ 又是可数个可数集的并集。再次应用定理1.1的系，我们导出 $\boldsymbol{Q}[x]$ 是可数集。▎

定理5.3 代数数的集合是可数的。

证明 先把 $\boldsymbol{Q}[x]$ 的非零元素排成一列：

$$f_1(x),\quad f_2(x),\quad \cdots,\quad f_n(x),\quad \cdots,$$

每个非零多项式只有有限多个根，于是

$$\text{代数数的集合}=\bigcup_{i=1}^{\infty}\{a:\ a\text{ 是 }f_i(x)\text{的根}\}.$$

这是可数个有限集的并集。应用定理1.1的系，我们导出这是一个可数集。▎

根据定理1.2，我们知道实数集 $\boldsymbol{R}$ 是一个不可数集。于是 $\boldsymbol{C}$ 也是不可数集。根据定义5.2，我们有

$$\boldsymbol{C}=\text{代数数的集合}\cup\text{超越数的集合},$$

故超越数的集合必然是不可数集。应用“测度论”与“概率论”的概念，任何可数集的测度皆为零。于是自 $\boldsymbol{C}$ 中任取一数 c，则 c 为代数数的概率为零，而 c 为超越数的概率为 1。在这种意义下，代数数是非常稀少的，而几乎所有的复数皆是超越数。然而如果给定一个数（例如圆周率 π 或自然对数 $\ln x$ 的底 e），则并不容易判定它是代数数，或是超越数。目前已知 π 及 e 皆为超越数，然而无人知道 $\pi+e,\pi-e,\pi e,\pi/e$ 等数是否为超越数。

习　题

1. 设$f(x)=(x-\mathrm{i})^2(x+1)^3$。证明存在$\boldsymbol{C}$上无穷多个5阶方阵$X$，使$f(X)=0$。

2. 设R是一个整环，包含$\boldsymbol{C}$为其子环，如果对R中的加法及$\boldsymbol{C}$与R中元素乘法，R组成$\boldsymbol{C}$上的有限维线性空间，则

$$R=\boldsymbol{C}.$$

3. 设$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n\in\boldsymbol{Z}[x]$，如果$f(0)$，$f(1)$都是奇数，证明$f(x)$无整数根。

4. 设$f(x)=x^n+a_1x^{n-1}+\cdots+a_n\in\boldsymbol{Z}[x]$，它的根都在单位圆内，证明它的根只能是单位根$\mathrm{e}^{2k\pi\mathrm{i}/m}$。

5. 设$f(x)=\sum\limits_{j=0}^{n}a_jx^{n-j}\in\boldsymbol{R}[x]$，它的根都是实数。证明

$$g(x)=\sum_{j=0}^{n}\binom{n}{j}a_jx^{n-j}$$

的根也都是实数。

6. 将复数域$\boldsymbol{C}$看作有理数域$\boldsymbol{Q}$上的线性空间，证明这个线性空间是无限维的。

7. 考察$\boldsymbol{C}$上如下二阶方阵所成集合：

$$\boldsymbol{H}=\left\{\begin{bmatrix}\alpha & \beta\\ -\bar{\beta} & \bar{\alpha}\end{bmatrix}:\ \alpha,\beta\in\boldsymbol{C}\right\}.$$

证明$\boldsymbol{H}$关于矩阵加法、乘法成一非交换环，其中每个非零元素都是可逆的。$\boldsymbol{H}$称为**四元数体**，它包含$\boldsymbol{C}$。

8. 续上题。令$\alpha=1$，$\beta=0$，得$\boldsymbol{H}$的元素E；令$\alpha=\mathrm{i}$，$\beta=0$，得I；令$\alpha=0$，$\beta=1$得J；令$\alpha=0$，$\beta=\mathrm{i}$得K。证明：

$$I^2=J^2=K^2=-E,$$

$$IJ=-JI=K,\ JK=-KJ=I,\ KI=-IK=J.$$

（请与第二章§1的习题7相对照。）

§2 代数扩域

在上一节中，我们提到两个域 $\mathbf{Q}, \mathbf{C}$ 有包含的关系。一般言之，设有两个域 $K \subset L$，而且其加法与乘法的定义是一致的，则称 K 是 L 的**子域**，L 是 K 的**扩域**。就像定义5.2一样，如 K 是 L 的子域时，我们可以定义"代数元"及"超越元"如下：

定义5.3 设 K 是 L 的子域。如果 L 的元素 α 能适合 $K[x]$ 中的某一非零的多项式 $f(x)$，即 $f(\alpha)=0$，则称 α 为(对 K 的)**代数元**。反之，如果 α 不是任何非零的多项式 $f(x)\in K[x]$ 的根，即如果 $f(x)\neq 0$，$f(\alpha)$ 恒不为零，则称 α 为(对 K 的)**超越元**。如果 L 的元素都是对 K 的代数元，则称 L 是 K 的**代数扩域**。

对于代数元，我们有下列的判定定理：

定理5.4 设 K 是 L 的子域，$\alpha\in L$，则下列四个条件等价：

1) α 是代数元；

2) $K[\alpha]=\{f(\alpha):\ f(x)\in K[x]\}$ 是有限维的 K 向量空间；

3) 环映射

$$\rho:\ K[x]\to K[\alpha],$$
$$\rho(g(x))=g(\alpha)$$

的核 $\rho^{-1}(0)=(f(x))\neq(0)$。$K[\alpha]$ 与 $K[x]/(f(x))$ 同构；

4) $K[\alpha]$ 是域。

于是，条件 2)，3)，4) 也是代数元的定义。

证明 采用循环证法：1) $\Longrightarrow$ 3) $\Longrightarrow$ 2) $\Longrightarrow$ 4) $\Longrightarrow$ 1)。

1) $\Longrightarrow$ 3)。不论 α 是否是代数元，条件 3) 中的映射 ρ 总是环满射。已知 α 是代数元，于是 $K[x]$ 中至少有一非零的多项式 $h(x)$，使 $h(\alpha)=0$，即 $\rho(h(x))=0$。于是 $h(x)\in\rho^{-1}(0)$，$\rho^{-1}(0)\neq(0)$。因为 $K[x]$ 是主理想环，而 $\rho^{-1}(0)$ 是一个理想，所以存在 $f(x)\in K[x]$，$f(x)\neq 0$，使 $\rho^{-1}(0)=(f(x))$。按照定理3.22，

$K[\alpha]$与$K[x]/(f(x))$同构。

3) $\Longrightarrow$ 2)。我们自然仅须证明$K[x]/(f(x))$是有限维K向量空间。设$n=\deg f(x)$，已知$f(x)$是非零多项式，于是$f(x)$必是非常数的多项式(因为如果$f(x)$是非零的常数，则$(f(x))=(1)=K[x]$，从而$K[x]/(f(x))=\{0\}$，不可能与$K[\alpha]$同构)。这样，我们有$\deg f(x)=n\geqslant 1$。以$\overline{g(x)}$表示$g(x)\in K[x]$在典型映射$K[x]\to K[x]/(f(x))$下的象，我们要证明$\{\bar{1},\bar{x},\bar{x}^2,\cdots,\bar{x}^{n-1}\}$是$K[x]/(f(x))$的一组基。如此，则知$K[x]/(f(x))$是$n$维$K$向量空间。

任取$\overline{g(x)}\in K[x]/(f(x))$。按照欧几里得算法，存在$d(x)$，$r(x)\in K[x]$，使

$$g(x)=d(x)f(x)+r(x), \qquad \deg r(x)<\deg f(x).$$

对上式作典型映射$K[x]\to K[x]/(f(x))$，则得出

$$\overline{g(x)}=\overline{d(x)}\ \overline{f(x)}+\overline{r(x)}=\overline{r(x)}=\sum_{i=0}^{n-1}a_i\bar{x}^i.$$

于是$\{\bar{1},\bar{x},\bar{x}^2,\cdots,\bar{x}^{n-1}\}$是生成元集。又如果有线性关系式

$$\sum_{i=0}^{n-1}a_i\bar{x}^i=0,$$

则有

$$\sum_{i=0}^{n-1}a_ix^i\in(f(x)), \qquad f(x)\,\Big|\,\sum_{i=0}^{n-1}a_ix^i.$$

比较$f(x)$与$\sum\limits_{i=0}^{n-1}a_ix^i$的次数，立得$\sum\limits_{i=0}^{n-1}a_ix^i$为零多项式，也即$a_i=0$ $(\forall i=0,1,\cdots,n-1)$。于是$\{\bar{1},\bar{x},\bar{x}^2,\cdots,\bar{x}^{n-1}\}$是线性无关集。综上所述，我们得出$\{\bar{1},\bar{x},\bar{x}^2,\cdots,\bar{x}^{n-1}\}$是$K[x]/(f(x))$的基。

2) $\Longrightarrow$ 4)。因为$K[\alpha]\subset L$，所以$K[\alpha]$自然是一个整环。要证明$K[\alpha]$是域，仅须证明对任意的$h(\alpha)\in K[\alpha]$，$h(\alpha)\neq 0$，则

$h(\alpha)$在$K[\alpha]$中皆有逆元。设$\dim_K K[\alpha]=n$，则$\{1,h(\alpha),h(\alpha)^2,\cdots,h(\alpha)^n\}$必为线性相关集。于是有一线性方程式

$$a_0+a_1h(\alpha)+\cdots+a_nh(\alpha)^n=0,$$

其中至少有一个$a_i\neq 0$。如果$a_0=0$，上式可写成

$$(a_1+a_2h(\alpha)+\cdots+a_nh(\alpha)^{n-1})h(\alpha)=0.$$

由于$K[\alpha]$是整环，$h(\alpha)\neq 0$，所以必有

$$a_1+a_2h(\alpha)+\cdots+a_nh(\alpha)^{n-1}=0.$$

如此逐步推论，不难看出必有一线性方程式

$$b_0+b_1h(\alpha)+\cdots+b_mh(\alpha)^m=0,$$

其中$b_0\neq 0$，$m\leqslant n$。上式又可改写成

$$1=-\left(\frac{b_1}{b_0}+\cdots+\frac{b_m}{b_0}h(\alpha)^{m-1}\right)h(\alpha),$$

于是证出$h(\alpha)$在$K[\alpha]$中有逆元。

4)$\Longrightarrow$1)。如果$\alpha=0$，则α是x的根，α自然是代数元。如果$\alpha\neq 0$，则α在$K[\alpha]$中有逆元，令其为$\sum_{i=0}^{l}a_i\alpha^i$。于是

$$\alpha\left(\sum_{i=0}^{l}a_i\alpha^i\right)=1,$$

即
$$a_l\alpha^{l+1}+\cdots+a_0\alpha-1=0.$$

令$f(x)=a_lx^{l+1}+\cdots+a_0x-1$，则$f(\alpha)=0$。又显然$f(x)\neq 0$，故知$\alpha$为代数元。▎

系 设K是L的子域，$\alpha\in L$，则下列四个条件是等同的：

1) α是超越元；

2) $K[\alpha]$是无限维K向量空间；

3) 环映射

$$\rho:\ K[x]\to K[\alpha],$$
$$\rho(g(x))=g(\alpha)$$

的核$\rho^{-1}(0)=(0)$，$K[\alpha]$与$K[x]$为自然同构；

4) $K[\alpha]$不是域。

于是，条件 2)，3)，4) 也是超越元的定义。

证明 系的条件 1)，2)，3)，4) 与定理 5.4 的条件 1)，2)，3)，4)恰好相反。 ▌

定理5.4的条件 3)给出如下的定理。

定理5.5 设 K 是 L 的子域，$\alpha\in L$，α 是代数元。则对一个非零的多项式 $f(x)\in K[x]$而言，下列两条件是等同的：

1) $f(\alpha)=0$，$f(x)$ 是 $K[x]$的不可约的多项式；

2) $(f(x))=\{g(x):\ g(x)\in K[x],\ g(\alpha)=0\}$。

如果要求 $f(x)$是首一多项式，则 $f(x)$是由上述条件唯一确定的. 此时称 $f(x)$为 α 的**极小多项式**，$f(x)$的次数称为 α (对 K 的)**代数次数**。

证明 1)$\Longrightarrow$2)。令

$$I=\{g(x):\ g(x)\in K[x],\ g(\alpha)=0\}.$$

显然，I 是一个理想. 我们已知 $K[x]$是一个主理想环，所以 $I=(h(x))$，其中 $h(x)$不是可逆的。由于 $f(\alpha)=0$，所以 $f(x)\in I$，故必有

$$f(x)\in(h(x)),\qquad h(x)\,|\,f(x).$$

而 $f(x)$是不可约的，于是立得

$$f(x)\,|\,h(x),\qquad I=(h(x))=(f(x)).$$

2)$\Longrightarrow$1)。根据定理 5.4 的条件 3)，我们有

$$K[\alpha]\approx K[x]/(f(x)).$$

由于 $K[\alpha]\subset L$，所以 $K[\alpha]$是一个整环。根据定理 3.24，立得 $(f(x))$是一个素理想. 读者不难看出，这就是说 $f(x)$是一个素元. 而在 $K[x]$中，素元即是不可约多项式，于是本定理得证. ▌

系 α 的代数次数即是 K 向量空间 $K[\alpha]$的维数.

证明 根据定理5.4的条件 3)，知

$$K[\alpha]\approx K[x]/(f(x)).$$

设 $\deg f(x)=n$，即 α 的代数次数为 n。在定理5.4的证明中已推出 $\{\bar{1},\bar{x},\bar{x}^2,\cdots,\bar{x}^{n-1}\}$ 是 $K[x]/(f(x))$ 的一组基，于是本系理得.

证。 ▌

定义5.4 设K是L的子域，用符号$[L:K]$表示L作为K向量空间的维数。如果$[L:K]<\infty$，则称L为K的有限扩域。

讨论： 如果$\alpha\in L\supset K$是(对K的)代数元，则$K[\alpha]$显然是K的有限扩域。反之，如果L是K的有限扩域，则对任意$\alpha\in L$，有

$$\infty>[L:K]\geqslant[K[\alpha]:K]=\dim_K K[\alpha].$$

于是$K[\alpha]$是有限维K向量空间。根据定理5.4，立得α是代数元以及$K[\alpha]$是域。于是$K[\alpha]$也是K的有限扩域。

定理5.6 设L是K的有限扩域，S是L的有限扩域，则恒有

$$[S:K]=[S:L][L:K].$$

于是S也是K的有限扩域。

证明 设$\{\alpha_1,\cdots,\alpha_n\}$是$L$向量空间$S$的一组基，$\{\beta_1,\cdots,\beta_m\}$是$K$向量空间$L$的一组基。我们要证明

$$\{\alpha_i\beta_j:\ i=1,\cdots,n,\ j=1,\cdots,m\}$$

是K向量空间S的一组基。

设有下列的线性关系式

$$\sum_{i,j}c_{ij}\alpha_i\beta_j=0,\qquad c_{ij}\in K.$$

则有

$$\sum_i\Big(\sum_j c_{ij}\beta_j\Big)\alpha_i=0,\qquad \sum_j c_{ij}\beta_j\in L.$$

因为$\{\alpha_1,\cdots,\alpha_n\}$是$L$线性无关的，于是得出

$$\sum_j c_{ij}\beta_j=0,\qquad \forall i=1,2,\cdots,n.$$

而$\{\beta_1,\cdots,\beta_m\}$是$K$线性无关的，于是得出

$$c_{ij}=0,\qquad \forall i=1,\cdots,n,\ j=1,\cdots,m.$$

如此，我们证明了$\{\alpha_i\beta_j:\ i=1,\cdots,n,\ j=1,\cdots,m\}$是$K$线性无关

的。

任取$\gamma\in S$，则有$d_1,\cdots,d_n\in L$，使

$$\gamma=d_1\alpha_1+\cdots+d_n\alpha_n.$$

又因$\{\beta_1,\cdots,\beta_m\}$是$K$向量空间$L$的基，于是存在$f_{ij}\in K(i=1,\cdots,n,\ j=1,\cdots,m)$，使$d_i=\sum_j f_{ij}\beta_j$。于是有

$$\gamma=\sum_{i,j}f_{ij}\alpha_i\beta_j,\qquad f_{ij}\in K.$$

这样，我们证明了$\{\alpha_i\beta_j:\ i=1,\cdots,n,\ j=1,\cdots,m\}$是$K$向量空间$S$的基。由此立得

$$[S:K]=nm=[S:L][L:K]. \quad \blacksquare$$

讨论 既使$[L:K]=\infty$或$[S:L]=\infty$，在集合论的基数的意义下，我们仍可以证明

$$[S:K]=[S:L][L:K].$$

上式的证明并不难，然而本书用不到这个结果，所以不给证明。读者不妨证证看。

定理5.7 1) 设L是K的扩域，$\alpha,\beta\in L$是对K的代数元。则有$K[\alpha,\beta]=K[\alpha][\beta]$是$K$的有限扩域。于是$\alpha\pm\beta,\alpha\beta,\alpha\beta^{-1}$ $(\beta\neq0)$皆是对K的代数元。L中所有对K的代数元的集合是K的扩域，称为**K在L中的代数闭包**，记为K_L^c。

2) 如果R是K的代数扩域，S是R的代数扩域，则S是K的代数扩域。又设R是L的子域，如果$R_L^c=R$，则称**R在L中是代数封闭的**。K_L^c在L中是代数封闭的。

证明 1) 因为β是对K的代数元，即β适合$K[x]$中的一个非零多项式$f(x)$。显然$f(x)\in K[x]\subset K[\alpha][x]$，于是$\beta$是对$K[\alpha]$的代数元。根据定理5.6，我们有

$$[K[\alpha,\beta]:K]=[K[\alpha][\beta]:K[\alpha]][K[\alpha]:K].$$

此式右侧的两个数皆是有限数，于是$K[\alpha,\beta]$是K的有限扩域。

显然，$\alpha,\beta,-\beta,\beta^{-1}(\beta\neq0)$皆在$K[\alpha,\beta]$中，于是$\alpha$与$\beta$作

加、减、乘、除(只要除法是有意义的)的结果都是代数元。于是K_L^c自然是域。又，如果$a\in K$，a适合$x-a\in K[x]$，故K的元素皆是对K的代数元。如此，$K\subset K_L^c$，于是K_L^c是K的扩域。

2) 设$\gamma\in S$。则有一非零的多项式

$$f(x)=\sum_{i=0}^{n}a_i x^i\in R[x],$$

使$f(\gamma)=0$。我们可以列出下面的域的链：

$$K\subset K[a_0]\subset K[a_0,a_1]\subset\cdots\subset K[a_0,a_1,\cdots,a_n]$$
$$\subset K[a_0,a_1\cdots,a_n,\gamma].$$

此链中的每个域(除了首项的K)皆是前一域的有限扩域。应用定理5.6，不难证出

$$[K[a_0,\cdots,a_n,\gamma]:K]=[K[a_0,\cdots,a_n,\gamma]:K[a_0,\cdots,a_n]]$$
$$\times\prod_{i=1}^{n}[K[a_0,\cdots,a_i]:K[a_0,\cdots,a_{i-1}]],$$

于是$K[a_0,\cdots,a_n,\gamma]$是K的有限扩域。由此得出γ是对K的代数元。故S是K的代数扩域。设$\gamma\in L$是对K_L^c的代数元，则γ是对K的代数元，于是$\gamma\in K_L^c$，即K_L^c在L中是代数封闭的。▌

系 如果L是K的扩域，而且L是代数封闭的(参见定义5.1)，则K在L中的代数闭包是代数封闭的。

证明 任取一个非常数的多项式$f(x)\in K_L^c[x]$，则$f(x)\in L[x]$。于是$f(x)$在L中有一根a。根据上定理的2)，$a\in K_L^c$。于是K_L^c是代数封闭的。▌

例1 根据上面的系理，$\mathbf{Q}$在$\mathbf{C}$中的代数闭包$\mathbf{Q}_C^c$，即所有代数数的集合，是一个代数封闭的域。根据定理5.3，此集合是一个可数集。

有一个流行的误解，认为从$\mathbf{Q}$扩充到$\mathbf{C}$是单纯为了解一元多项式。从上一段的论述中可以看出，如果单纯为了解一元多项式，应该从$\mathbf{Q}$扩充到$\mathbf{Q}_C^c$。其实，数论是从$\mathbf{Q}$先扩充到$\mathbf{R}$，这一

步是求 **Q** 的“完备化集”（见第一章§6），如此得出 **R**。然后再求解实数方程式，才得到 **C**。∎

定理5.5定义了一个代数元 α 的极小多项式 $f(x)\in K[x]$，它是 α 适合的不可约的首一多项式。如果域是代数封闭的，则不可分解的多项式皆是一次式。在一般情况下，如何判别一个多项式是否是不可分解的？这是一个相当棘手的问题。下面这个定理，提供了相当有效的部分解答。

爱森斯坦判别定理 设 R 是一个唯一分解的整环，K 是 R 的比域（参见定义3.6），$f(x)\in R[x]\subset K[x]$。如果在 R 中存在素元 p，使得在 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$ 中有

$$p\nmid a_0,\quad p\mid a_i\quad(i=1,\cdots,n),$$

$$p^2\nmid a_n,\quad n\geqslant 1,$$

则 $f(x)$ 是 $K[x]$ 的不可分解的多项式。

证明 令 $f(x)$ 的内涵为 $C(f(x))$（参见定义3.13）。取 $d\in C(f(x))$。令

$$f(x)=df^*(x),\quad f^*(x)=a_0^*x^n+a_1^*x^{n-1}+\cdots+a_{n-1}^*x+a_n^*.$$

显然，d 在 K 中是可逆元，而且 $p\nmid d\mid a_0$。不难看出，我们依然有 $f^*(x)\in R[x]\subset K[x]$ 以及

$$p\nmid a_0^*,\quad p\mid a_i^*\quad(i=1,\cdots,n),$$

$$p^2\nmid a_n^*.$$

如能证明 $f^*(x)$ 是 $K[x]$ 的不可分解的多项式，则 $f(x)$ 也是 $K[x]$ 的不可分解的多项式。如此，我们不妨设 $f(x)=f^*(x)$，即 $f(x)$ 是一个本原多项式。

根据定理3.12，我们仅须证明 $f(x)$ 是 $R[x]$ 的不可分解的多项式。假设 $f(x)$ 在 $R[x]$ 中可以分解为

$$f(x)=g(x)h(x),\quad \deg g(x)\geqslant 1,\ \deg h(x)\geqslant 1.$$

令 ρ: $R[x]\to(R/(p))[x]$ 为自然的映射。又令 S 为 $R/(p)$ 的比域，则在 $S[x]$ 中有下列等式

$$\rho(f(x))=\rho(a_0)x^n=\rho(g(x))\rho(h(x)).$$

因为 $\rho(a_0)\neq 0$，而且 S 是唯一分解的整环，于是必有

$$\rho(g(x))=b_1x^m,\quad \rho(h(x))=b_2x^{n-m}.$$

如此立得 $\rho(g(0))=0=\rho(h(0))$，即

$$p\mid g(0),\quad p\mid h(0).$$

不难看出，我们得到了一个如下的矛盾：

$$p^2\mid g(0)h(0)=f(0)=a_n. \quad \blacksquare$$

例 2 古希腊的数学家起初相信每一个实数都是有理数。取两个直角边长度均为 1 的直角三角形，应用商高定理（即毕氏定理）立得其弦长是 $\sqrt{2}$。当时证明了 $\sqrt{2}$ 不是有理数，于是得出了 $\sqrt{2}$ 是一个数(实数)又不是一个数(有理数)的奇异难懂的矛盾。中国的古数学是向小数进位的方向发展，读者可以参考"九章算术"，所以没有产生这个问题。

我们可用上述定理证明 $\sqrt{2}$ 不是有理数。令 $f(x)=x^2-2$，$p=2$，$R=\boldsymbol{Z}$，$K=\boldsymbol{Q}$，则立得 $f(x)$ 是不可分解的首一多项式，以及 $f(x)$ 是 $\sqrt{2}$ 的极小多项式。如此，$\sqrt{2}$ 的代数次数是

$$\deg f(x)=2.$$

于是 $\boldsymbol{Q}(\sqrt{2})\supsetneqq\boldsymbol{Q}$，即 $\sqrt{2}\notin\boldsymbol{Q}$，也即 $\sqrt{2}$ 不是有理数。同理，设 $\alpha\in\boldsymbol{Z}$，

$$\alpha=p^{mn+1}\beta,$$

其中 p 为素数，$p\nmid\beta$，$m>1$，n 为任意的整数。令

$$\gamma=\alpha/p^{mn}.$$

则同理可知，$g(x)=x^m-\gamma$ 是不可分解的首一多项式。于是 $\sqrt[m]{\gamma}$ 不是有理数，所以 $\sqrt[m]{\alpha}=p^n\sqrt[m]{\gamma}$ 也不是有理数。

例3 设 p 为素数。令 $\varphi_p(x)$ 为"p 次割圆多项式"，即

$$\varphi_p(x)=(x^p-1)/(x-1)=x^{p-1}+x^{p-2}+\cdots+1.$$

在复数平面 $\boldsymbol{C}$ 上，$\varphi_p(x)$ 的根的集合即是在单位圆上以 1 为一顶点的正 p 边形的其余 $p-1$ 个顶点的集合。图5.1表示了 $p=5$ 的情形。

我们要证明 $\varphi_p(x)$ 是不可分解的多项式。令 $y = x - 1$，则有

$$
\begin{aligned}
\varphi_p(y+1) &= ((y+1)^p - 1)/y \\
&= y^{p-1} + p y^{p-2} + \cdots + \binom{p}{i} y^{p-i-1} + \cdots + p.
\end{aligned}
$$

因为 p 为素数，所以不难证出

$$
p \,\Big|\, \binom{p}{i}, \qquad i = 1, 2, \cdots, p-1,
$$

$$
p^2 \nmid p,
$$

于是 $\varphi_p(x) = \varphi_p(y+1)$ 是不可分解的多项式(参见上定理)。

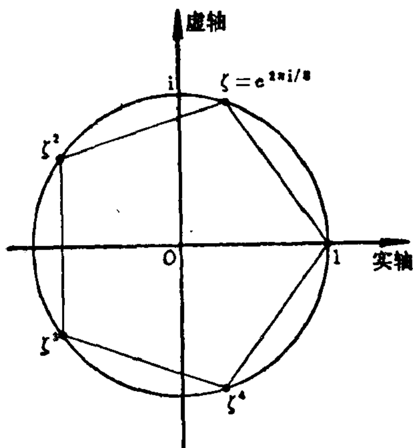
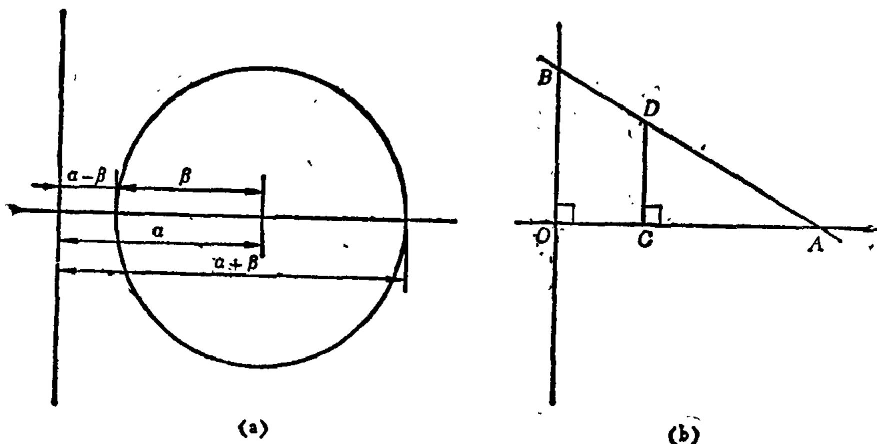


图 5.1

例 4 古希腊的数学家对圆与直线有偏爱，于是产生了用圆规及直尺作图的问题。作图的规则如下：在平面上任取一直线为基准。在此直线上任取一原点及一单位长，然后以原点为圆心，单位长为半径画圆，与基准线相交，取得新的交点，即 ±1。如此逐步作下去，每次可以用已作出的点，或作为圆心，或通过已作出的两点画出一条直线。在画圆时，只能用已经作出的两个点之间的

距离为半径。在这种规则限制下，什么图形可以作出来呢？什么图形作不出来呢？

我们可以把这个平面当作复数平面，这个基准线当作实数轴 x，原点即 O 点，单位长度即 1。从平面几何学中，我们知道通过原点可以作 x 轴的垂线，如此得出虚数轴 y，如果两个长度 α,β 已经作出，我们来证明 $\alpha\pm\beta,\alpha\beta$ 及 $\beta^{-1}(\beta\neq0)$ 都能作出。请看图 5.2的图(a)和图(b)。易见图(a)中作出了 $\alpha\pm\beta$。在图(b)中，$\triangle OAB\backsim$



(a)　　(b)

图 5.2

$\triangle CAD$。如果取 $\overline{OA}=\alpha$，$\overline{CA}=1$，$\overline{CD}=\beta$，则立得 $\overline{OB}=\alpha\beta$。又如果取 $\overline{OB}=1=\overline{CA}$，$\overline{OA}=\beta$，则立得 $\overline{CD}=\beta^{-1}$。

我们很容易把上面的讨论推广到复数的情形，一个复数 $\gamma=\alpha+\beta i$ 对应到平面上的点 (α,β)。不难看出，γ 可以作出 $\Longleftrightarrow\alpha$ 和 β 可以作出。如果 $\gamma_1=\alpha_1+\beta_1 i$，$\gamma_2=\alpha_2+\beta_2 i$ 为已经作出的，则

$$\gamma_1\pm\gamma_2=(\alpha_1\pm\alpha_2)+(\beta_1\pm\beta_2)i,$$

$$\gamma_1\gamma_2=(\alpha_1\alpha_2-\beta_1\beta_2)+(\alpha_1\beta_2+\alpha_2\beta_1)i$$

以及 $\gamma_1^{-1}=(\alpha_1-\beta_1 i)/(\alpha_1^2+\beta_1^2)(\gamma_1\neq0)$ 都能作出。

让我们从头开始考虑作图问题。首先我们有单位长 1，于是

根据以上的讨论，我们可以在实数轴及虚数轴上，作出Q及Qi。如此，域$Q[i]$的任一元素皆可作出。同理，如作出α后，则域$Q[i](\alpha)$的任意元素都可作出.我们可以把以上的讨论推而广之。设经过有限步骤作图以后，我们已知Q的扩域K的元素都可以作出，又知另有一复数γ也可以作出，则我们导出Q的扩域$K(\gamma)$的元素皆可以作出。

从上面的讨论，我们看出，圆规直尺作图的问题即是从域K到扩域$K(\gamma)$的问题。我们想要弄清楚，在圆规直尺的限制下，可以作出的复数γ将会受到什么代数性的限制。

设我们已知域K的元素都能作出（此处K自然可能是Q），在仅能用K中的复数点和实数长时，我们能作出什么样的新的复数点和实数长呢？应用圆规与直尺，我们有三种可能的情形：直线与直线相交；直线与圆相交；圆与圆相交。

1）直线与直线相交。设此二直线的方程为

$$(\alpha_1-\alpha_2)(y-\beta_2)=(\beta_1-\beta_2)(x-\alpha_2),$$

$$(\alpha_3-\alpha_4)(y-\beta_4)=(\beta_3-\beta_4)(x-\alpha_4),$$

其中$\alpha_1+\beta_1 i,\alpha_2+\beta_2 i,\ \alpha_3+\beta_3 i,\alpha_4+\beta_4 i\in K$，$\alpha_j,\beta_j$都是实数。不难看出，上两个方程的公解在$K$中，于是直线与直线相交不会得出新的点，也没有新的实数长。

2）直线与圆相交。令此直线及圆的方程为

$$(\alpha_1-\alpha_2)(y-\beta_2)=(\beta_1-\beta_2)(x-\alpha_2),$$

$$(x-\alpha_3)^2+(y-\beta_3)^2=c^2,$$

此处α_j,β_j，c都是实数，$c,\alpha_1+\beta_1 i,\alpha_2+\beta_2 i,\alpha_3+\beta_3 i\in K$。把线性方程式代入二次式，得出一个一元二次多项式。此多项式或可分解，或不可分解。相应地，此元（x或y）的解的代数次数是1或2。又可用线性方程式求解另一元。总上所论，直线与圆的交点γ或在K中，或$K[\gamma]$是K的二次扩域。如果得出不在K中的新交点后，则此新点与其它点的距离，应用商高定理，又不外乎在$K[\gamma]$的一个二次扩域内。

3）两圆相交．令此二圆的方程式为

$$(x-\alpha_1)^2+(y-\beta_1)^2=c_1^2,$$

$$(x-\alpha_2)^2+(y-\beta_2)^2=c_2^2,$$

此处 α_j,β_j,c_j 都是实数，$c_1,c_2,\alpha_1+\beta_1\mathrm{i},\alpha_2+\beta_2\mathrm{i}\in K$．将上面两式相减，得出一线性方程式

$$\alpha_3x+\beta_3y=c_3.$$

显然 α_3,β_3,c_3 都是实数，且在 K 中．这个线性方程式可以理解成通过已作出的两个点的直线．所以，两圆相交的情形可以归结成直线与圆相交的情形，讨论见 2）．

综上所述，一个复数点或实数长 γ，能以有限步骤作图得出的必要条件，是存在一个二次扩域的链：

$$\boldsymbol{Q}\subset K_1\subset\cdots\subset K_j\subset\cdots K_n,$$

$$[K_1:\boldsymbol{Q}]=2,\qquad [K_j:K_{j-1}]=2,$$

使 $\gamma\in K_n$．反之，我们要证明这个必要条件也是充分条件．

我们仅须证明，如果 K_{j-1} 的元素皆可作出，$[K_j:K_{j-1}]=2$，则 K_j 的元素皆可作出．任取 $\gamma\in K_j$，不妨设 γ 对 K_{j-1} 的代数次数是 2．令其极小多项式为

$$x^2+\alpha x+\beta=0,\qquad \alpha,\beta\in K_{j-1}.$$

令 $y=x+\alpha/2$，则有

$$y^2=\frac{1}{4}\alpha^2-\beta.$$

如果 $(\alpha^2/4)-\beta\geqslant0$，则 y 自然是实数，如果 $(\alpha^2/4)-\beta<0$，则 y 是纯虚数．两者的差别不过是在实数轴或虚数轴取值而已．所以不妨即假设 $(\alpha^2/4)-\beta\geqslant0$．用相似三角形的各边的比例关系，读者即可以利用图 5.3 求出

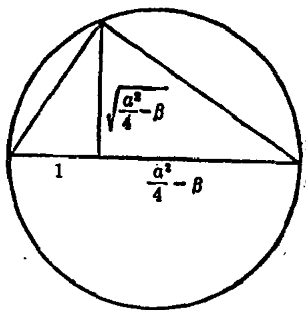


图 5.3

$\sqrt{(\alpha^2/4)-\beta}$。如此，

$$\gamma=-\frac{\alpha}{2}\pm\sqrt{\frac{1}{4}\alpha^2-\beta}$$

也可以作出。我们证明了上述的必要条件也是充分条件。

例 5 应用上面例 4 的讨论，我们可以解决古希腊的数学难题：任意角能不能三等分？上面的提法不够精确，精确的提法是：任意能用圆规直尺作出的角，能不能用圆规直尺作图进行三等分？

我们用三角学的公式可以导出

$$4\cos^3\theta-3\cos\theta=\cos 3\theta.$$

令 $\theta=20^\circ$，则 $3\theta=60^\circ$。众所周知，60° 角是可以用圆规直尺作出的。假如60°角可以三等分，则20°角与单位圆的交点$(\cos 20^\circ, \sin 20^\circ)$ 也可用圆规直尺作出。由上式导出 $\cos 20^\circ$ 适合下面的方程：

$$(1)\qquad 4x^3-3x=\frac{1}{2}.$$

令$x=(y+1)/2$，代入上式，化简后，即得

$$(2)\qquad y^3+3y^2-3=0.$$

根据爱森斯坦判别定理，(2)式左侧不可分解，于是，将(1)式中的1/2移项后，其左侧也不可分解。由此即知 $\cos 20^\circ$对 $\boldsymbol{Q}$ 的代数次数是 3。如果 $\cos 20^\circ$可以作出，则存在一个二次扩域的链：

$$\boldsymbol{Q}\subset K_1\subset\cdots\subset K_n,$$

使 $\cos 20^\circ\in K_n$。根据定理5.6，不难看出

$$[K_n:\boldsymbol{Q}]=2^n,$$

$$2^n=[K_n:\boldsymbol{Q}]=[K_n:\boldsymbol{Q}[\cos 20^\circ]][\boldsymbol{Q}[\cos 20^\circ]:\boldsymbol{Q}]=l\times 3,$$

此处 l 是整数。显然不能有 $2^n=l\times 3$。于是60°角不能用圆规直尺作图法三等分。

例6 设 p 是素数，$p>2$。能不能用圆规直尺作图法作出单位圆的内接正 p 边形呢？不妨假设此正 p 边形的一个顶点是 1，其余的顶点依次为 $\zeta,\zeta^2,\cdots,\zeta^{p-1}$。根据例3的讨论，$\zeta$ 对 $\boldsymbol{Q}$ 的极小多项式是

$$\varphi_p(x)=x^{p-1}+x^{p-2}+\cdots+1.$$

于是 ζ 对 $\boldsymbol{Q}$ 的代数次数是 $p-1$。如果 ζ 可以用圆规直尺作出，则根据例4的讨论，必有一个二次扩域的链：

$$\boldsymbol{Q}\subset K_1\subset\cdots\subset K_n,\quad \zeta\in K_n.$$

于是得出

$$2^n=[K_n:\boldsymbol{Q}]=[K_n:\boldsymbol{Q}[\zeta]][\boldsymbol{Q}[\zeta]:\boldsymbol{Q}]=l(p-1),$$

所以必有

$$p-1=2^m,\quad p=2^m+1.$$

如果 m 有一奇因子 $s>1$，令 $m=sr$，则有

$$\begin{aligned}p&=2^m+1=(2^r)^s+1\\&=(2^r+1)((2^r)^{s-1}-(2^r)^{s-2}+\cdots-2^r+1),\end{aligned}$$

即 p 不是素数。所以，我们得知 m 无奇因子。设 $m=2^q$，即有 $p=2^{2^q}+1$。形如 $2^{2^q}+1$ 的素数称为**费马素数**。我们证出了能用圆规直尺作出单位元的内接正 p 边形（p 为素数）的必要条件是 p 为费马素数。以后我们将证明这也是充分条件。

在 $2^{2^q}+1$ 中，令 $q=0,1,2,3,4$，得出

$$3,\quad 5,\quad 17,\quad 257,\quad 65537.$$

这五个数都是素数。这也是仅知的五个费马素数。当 $q=5,6,7,8,9$ 时，则相应的 $2^{2^q}+1$ 都不是素数，以下也似乎并无素数了，然而无人能确定是否如此。

习　题

1. 设 k 是域，x 是变数。求 x 所满足的 $k\left(\dfrac{x^3}{x+1}\right)$ 上的不可约多项式。

2. 设 $x^4+1=0$ 的一个根为 ω，试将 x^4+1 在 $\mathbf{Q}[\omega]$ 内分解成不可约多项式之积。

3. 求域 $\mathbf{Q}[\mathrm{i},\sqrt{2}]$ 对有理数域 $\mathbf{Q}$ 的扩张次数。

4. 设 α 是 x^3-2 的一个零点，试问 $\mathbf{Q}[\alpha]$ 是否包含 x^3-2 的一切零点？

5. 证明 $\alpha=\mathrm{e}^{2\pi\mathrm{i}/8}$ 满足 $\mathbf{Q}[\mathrm{i}]$ 上的一个二次不可约多项式。

6. 设 $\alpha=\cos\frac{\pi}{6}+\mathrm{i}\sin\frac{\pi}{6}$，求 α 在 $\mathbf{Q}$ 上的极小多项式。

7. 设 α 是方程式 $x^3-x^2+x+2=0$ 的一个根，试将 $(\alpha^2+\alpha+1)(\alpha^2-\alpha)$ 及 $1/(\alpha-1)$ 表示成下列形式：

$$a\alpha^2+b\alpha+c \quad (a,b,c\in\mathbf{Q}).$$

8. 设 α 是域 K 上一奇数次不可约多项式的根，$L=K[\alpha]$。证明 $L=K[\alpha^2]$。

9. 设 $p_1,p_2,\cdots,p_n$ 是 n 个两两不等的素数，试求

$$[\mathbf{Q}[\sqrt{p_1},\sqrt{p_2},\cdots,\sqrt{p_n}]:\mathbf{Q}].$$

10. 设 K,L 是 $\mathbf{Q}$ 的两个有限次扩域，令

$$F=\left\{\sum_{\text{有限}}k_il_i:\ k_i\in K,\ l_i\in L\right\}.$$

证明 F 是 $\mathbf{Q}$ 的一个扩域，而且是包含 K,L 的最小扩域。

11. 设 K 是一个域，$L_1,L_2,\cdots$ 是 K 的扩域，且 $K\subset L_1\subset L_2\subset\cdots$。证明 $\bigcup_{i=1}^{+\infty}L_i$ 也是 K 的一个扩域。

12. 设 K 是域，x^n-a 在 $K[x]$ 内不可约，α 是 x^n-a 的一个根，$m|n$。证明 α^m 满足 K 上一个 n/m 次不可约多项式。

13. 设 F 是域 K 的代数扩域，R 是一整环，$K\subset R\subset F$。证明 R 是域。

14. 设 E_1,E_2 是 K 的子域，$\alpha\in K$。如果 E_1 的每个元素是 E_2 上的代数元，证明 $E_1[\alpha]$ 的每个元素是 $E_2[\alpha]$ 上的代数元。

15. 设 k 是域，x 是变数．$f(x),g(x)\in k[x]$ 且 $(f,g)=1$．又设

$$\max\{\deg f(x),\deg g(x)\}=n\geqslant 1.$$

求证

$$[k(x):k(f(x)/g(x))]=n.$$

§3. 代数闭包

设多项式 $f(x)\in \mathbf{Q}[x]$，我们可以在 $\mathbf{C}$ 中讨论 $f(x)$ 的根。如果取任意的域 K 及 $f(x)\subset K[x]$，我们如何讨论 $f(x)$ 的根呢？$f(x)$ 的根在什么地方呢？我们给出下面的定义。

定义5.5 设 L 是 K 的扩域。如果 L 的元素都是对 K 的代数元，即 L 是 K 的代数扩域，而且 L 是代数封闭的，则称 L 是 K 的**代数闭包**。

显然，在 K 的代数闭包 L 中，可以把 $f(x)\in K[x]\subset L[x]$ 完全分解(定理5.1)，也即可以考虑 $f(x)$ 的所有的根。给定域 K 以后，我们首先要证明可以构造它的代数闭包。先证明下面两个定理。

定理5.8 设 K 是域，$f(x)\in K[x]$ 为非常数的不可约的多项式。令 ρ: $K[x]\to K[x]/(f(x))$ 是典型映射，$\bar{x}=\rho(x)$。则恒有

1) $K[x]/(f(x))=K[\bar{x}]$ 是 K 的代数扩域，

$$[K[\bar{x}]:K]=\deg f(x);$$

2) $f(\bar{x})=0$，即 $f(x)$ 在 $K[\bar{x}]$ 中有根。

证明 在 $K[x]$ 中不可约的非常数的多项式即是 $K[x]$ 的素元。于是，$(f(x))$ 是 $K[x]$ 的素理想，$K[x]/(f(x))$ 是整环。令 L 为 $K[x]/(f(x))$ 的比域，则 $\bar{x}\in L$。显然，

$$K[x]/(f(x))=K[\bar{x}],\qquad \dim_K K[\bar{x}]=\deg f(x)<\infty.$$

根据定理5.4，即知 $K[\bar{x}]$ 是域，也是 K 的代数扩域，而且

$$[K[\bar{x}]:K]=\deg f(x).$$

于是1)得证. 又因为

$$0=\rho(f(x))=f(\rho(x))=f(\bar{x}),$$

所以本定理得证. ▎

定理5.9 设$\sigma: K\to K'$是域K到K'的同构. $f(x)\in K[x]$是一个非常数的不可约的多项式. σ可以自然地扩张成为一个环同构

$$\sigma: K[x]\to K'[x],$$
$$\sigma\left(\sum_i a_i x^i\right)=\sum_i \sigma(a_i)x^i.$$

设在K的扩域L中, $f(x)$有根α, 以及在K'的扩域L'中, $\sigma(f(x))$有根β. 则σ可以扩张成同构$\hat{\sigma}$: $K[\alpha]\to K'[\beta]$, 使

$$\hat{\sigma}(\alpha)=\beta.$$

证明 我们先证$\sigma(f(x))\in K'[x]$也是非常数的不可约的多项式. 假若$\sigma(f(x))=g(x)\cdot h(x)$, $g(x)$与$h(x)$为$K'[x]$中次数大于零的多项式, 则立得

$$f(x)=\sigma^{-1}\sigma(f(x))=\sigma^{-1}(g(x))\sigma^{-1}(h(x)).$$

这显然与$f(x)$是不可约的条件相违背.

根据定理5.4, 我们知道

$$K[\alpha]\approx K[x]/(f(x)), \quad \alpha\mapsto\bar{x},$$
$$K'[\beta]\approx K'[x]/(\sigma(f(x))), \quad \beta\mapsto\bar{x},$$

而且这两个同构是自然的. 把σ扩张成$\sigma: K[x]\to K'[x]$后, 我们有一个自然的同构

$$\sigma((f(x)))=(\sigma(f(x))).$$

于是不难看出, σ引生一个同构

$$K[x]/(f(x))\approx K'[x]/(\sigma(f(x))).$$

把上面几个同构连结在一起, 就有

$$\begin{array}{ccccccc} K[\alpha] & \approx & K[x]/(f(x)) & \approx & K'[x]/(\sigma(f(x))) & \approx & K'[\beta], \\ \alpha & \longmapsto & \bar{x} & \longmapsto & \bar{x} & \longmapsto & \beta. \end{array}$$

于是本定理得证。∎

任给一个域K，我们现在可以证明K的代数闭包的存在性及其在同构意义下的唯一性了。

定理5.10 设K是域。则存在K的一个代数闭包Ω。如果任给K的另一个代数闭包Ω'，则存在K同构$\sigma: \Omega \to \Omega'$（$\sigma$是$K$同构意即：$\sigma$是同构，而且$\sigma$在$K$上是恒等映射，即$\sigma(a)=a$，$\forall a\in K$）。

证明 我们要用Zorn引理。令

$S=\{(R,\sigma,R')$：R,R'是K的代数扩域，σ是R到R'的环单射，并且σ在K上是恒等映射$\}$。

显然，$(K,\mathrm{id},K)\in S$，这里id是恒等映射.所以S是非空集合。

在S里定义半序“$\leqslant$”如下：给定$(R_1,\sigma_1,R_1'),(R_2,\sigma_2,R_2')\in S$，$(R_1,\sigma_1,R_1')\leqslant(R_2,\sigma_2,R_2') \Longleftrightarrow R_1\subset R_2$，$R_1'\subset R_2'$，$\sigma_2$在$R_1$上等于$\sigma_1$。不难看出“$\leqslant$”确实是一个半序。

我们现在来检验Zorn引理的条件。设$\{(R_i,\sigma_i,R_i'): i\in I\}$是一个链。我们要证明此链有上限。令

$$\bar{R}=\bigcup R_i,\quad \bar{R}'=\bigcup R_i'.$$

再定义$\bar{\sigma}=\bigcup\sigma_i$如下：任取$r\in\bar{R}=\bigcup R_i$，则存在$i$，使$r\in R_i$，即令$\bar{\sigma}(r)=\sigma_i(r)$。根据链的定义，不难看出上面的$\bar{\sigma}$的定义是良好的：即设$r\in R_i$及$r\in R_j$，则有

$$(R_i,\sigma_i,R_i')\leqslant(R_j,\sigma_j,R_j') \text{ 或 } (R_j,\sigma_j,R_j')\leqslant(R_i,\sigma_i,R_i'),$$

不妨假设为前者。于是σ_j在R_i上等于σ_i，即有

$$\sigma_j(r)=\sigma_i(r).$$

所以$\bar{\sigma}$的定义是良好的。

易见$\bar{R}$及$\bar{R}'$都是K的代数扩域以及$\bar{\sigma}$是环映射。我们说明$\bar{\sigma}$是环单射。设有$r\in\bar{R}$，使$\bar{\sigma}(r)=0$。选取i，使$r\in R_i$，于是有

$$\sigma_i(r)=\bar{\sigma}(r)=0.$$

因为σ_i是环单射，故有$r=0$。这就证明了$\bar{\sigma}$是环单射。因此

$(\bar{R},\bar{\sigma},\bar{R}')\in S$ 是这个链的上限。于是 Zorn 引理的条件被验证了。

根据 Zorn 引理，我们知道 S 中存在一极大元素 (L,σ',L')。我们要证明 L' 是 K 的代数闭包，如此就证明了 K 的代数闭包的存在性。

如果 L' 不是 K 的代数闭包，则存在不可分解的多项式 $f(x)\in L'[x]$，$\deg f(x)>1$（参见定理5.1）。根据定理5.8，

$$\bar{L}=L'[x]/(f(x))$$

是 L' 的代数扩域，且 $\bar{L}\neq L'$。根据定理5.7，$\bar{L}$ 是 K 的代数扩域。不难看出，

$$\sigma:\ L\to L'\subset \bar{L}$$

是 L 到 $\bar{L}$ 的环单射。于是，$(L,\sigma,\bar{L})\in S$，且有

$$(L,\sigma,L')\leqslant(L,\sigma,\bar{L}),\qquad (L,\sigma,L')\neq(L,\sigma,\bar{L}),$$

这与 (L,σ,L') 是 S 的极大元素相矛盾。于是，L' 必然是代数封闭的。L' 自然是 K 的代数扩域，按照定义5.5，L' 是 K 的代数闭包。

设 Ω 和 Ω' 是 K 的两个代数闭包，我们要证明 Ω 与 Ω' 是 K 同构的。初始的步骤，与前面的讨论几乎完全一样。我们先把 S 的定义略加改变成为另一个集合 S' 的定义：

$$S'=\{(R,\sigma,R'):\ R,R'\text{是 }K\text{ 的代数扩域，}\ R\subset\Omega,\ R'\subset\Omega',\ \sigma\text{ 是 }R\to R'\text{ 的环单射，并且 }\sigma\text{ 在 }K\text{ 上是恒等映射}\}.$$

同法定义半序“$\leqslant$”以及检验 S' 适合 Zorn 引理的条件。于是根据 Zorn 引理，S' 有一极大元素 (L_*,σ,L'_*)。与上面完全一样，我们可以证明 L'_* 是 K 的代数闭包。而且容易看出 Ω' 是 L'_* 的代数扩域，但 L'_* 是代数封闭的，于是必有 $L'_*=\Omega'$。

以下我们要证明 L_* 也是代数封闭的，于是可以导出 $L_*=\Omega$。如果 L_* 不是代数封闭的，则存在不可约的多项式

$$f(x)\in L_*[x],\qquad \deg f(x)>1.$$

显然，σ：$L_* \to \sigma(L_*)$是域 L_* 到域 $\sigma(L_*)$的同构。σ 可以自然地扩张成同构 σ：$L_*[x] \to \sigma(L_*)[x]$。我们要应用定理5.9。因为 Ω 及 Ω' 都是代数封闭的，所以 $f(x)$ 及 $\sigma(f(x))$ 在 Ω 及 Ω' 中有根，令其为 α 及 β。于是 σ 可以扩张成$\hat{\sigma}$：

$$\hat{\sigma}: L_*[\alpha] \to \sigma(L'_*)[\beta] \subset L'_* = \Omega'.$$

不难看出，$(L_*[\alpha], \hat{\sigma}, L_*) \in S'$，以及

$$(L_*, \sigma, L'_*) \leqslant (L_*[\alpha], \hat{\sigma}, L'_*),$$

$$(L_*, \sigma, L'_*) \neq (L_*[\alpha], \hat{\sigma}, L'_*).$$

这与(L_*, σ, L'_*)是 S' 的极大元素相矛盾。于是 L_* 必是代数封闭的，以及 $L_* = \Omega$。

自然，$\sigma(\Omega) \subset \Omega'$，$\Omega'$是 $\sigma(\Omega) \supset K$ 的代数扩域，而且二者都是代数封闭的，立得

$$\sigma(\Omega) = \Omega',$$

即 σ 是 Ω 到 Ω' 的K 同构。▎

习　题

1. 证明 $\mathbf{Q}$ 的代数闭包$\overline{\mathbf{Q}}$ 不是 $\mathbf{Q}$ 的有限次扩域。

2. $\mathbf{Q}(\mathrm{i})$的代数闭包与$\overline{\mathbf{Q}}$ 是否相同？为什么？

3. 设域 k 的代数闭包为 $\bar{k}$，F 是 k 的一个代数扩域，证明在 $\bar{k}$ 内存在一个域 L，使 $k \subset L \subset \bar{k}$，且存在 L 到 F 的一个保持 k 的元素不动的同构映射。

4. 设 p 是一个素数，试求 $\mathbf{Q}_p$ 的一个扩域 K，使 K 包含 $\mathbf{Q}_p$ 上方程 $x^2+1=0$ 的所有根。

5. 试求 $\mathbf{Q}$ 上有理函数域 $\mathbf{Q}(x)$的一个扩域，使它包含 $\mathbf{Q}(x)$ 上多项式

$$y^2 - \frac{x^3}{x^2+1}$$

的一个根。

6. 设 K 是域，考虑 $K[x, y]$内不可约多项式

$$f(x,y)=a_0(x)y^n+a_1(x)y^{n-1}+\cdots+a_n(x) \quad (n\geqslant 1).$$

定义 $K(x)$到 $R=K[x,y]/(f(x,y))$的比域 L 的映射如下：

$$\sigma: \frac{f(x)}{g(x)} \mapsto \frac{f(\bar{x})}{g(\bar{x})}$$

(其中 $\bar{x}$ 表示R内的元素 $x+(f(x,y))$).证明 $\sigma(K(x))$是 L 的子域，与 $K(x)$同构。如把 $f(\bar{x},y)$看作 $\sigma(K(x))$上一个变元 y 的多项式，证明它在 L 内有一个根。

7. 设 $f(x)$是 $Q[x]$内一个 n 次不可约多项式，$\alpha_1,\alpha_2,\cdots,\alpha_n$ 是它在 C 内的 n 个根。证明域 $Q[\alpha_1],Q[\alpha_2],\cdots,Q[\alpha_n]$ 都同构于域 $Q[x]/(f(x))$。

§4 特征数及有限域

在代数学里，有许多不同的域。我们要把这些域分类。对于一个域K，我们要定义K的“特征数”或“特征”。在域K中，有一个唯一确定了的乘法的幺元，令其为$\bar{1}$。我们定义映射 σ: $Z\to K$ 如下：

$$\sigma(0)=0, \qquad \sigma(1)=\bar{1},$$

$$\sigma(n)=\overbrace{\bar{1}+\bar{1}+\cdots+\bar{1}}^{n\text{个}}, \qquad \sigma(-n)=-\sigma(n).$$

令 $\sigma^{-1}(0)=(p)$，此处要求 $p\geqslant 0$，我们定义K的特征数为 p。特征数也简称为特征。以下我们把 $\bar{1}$ 简记为 1。

映射 σ 引生一个单射 $\bar{\sigma}$: $Z/(p)\to K$。K 是一个整环，所以 $Z/(p)$也必是一个整环。于是 p 为零或素数。如果 p 是素数，$Z_p=Z/(p)$是一个域。将 Z_p 与 $\bar{\sigma}(Z_p)$ 认同以后，不妨即设 $K\supset Z_p$。如果K的特征是零，将 Z 与 $\sigma(Z)$认同以后，不妨即设$K\supset Z$。此时域K显然包含 Z 的比域 Q。

定义5.6 Q 及 Z_p，此处 p 为任意素数，称为素域。

定理5.11 设K的特征是零，则 $K\supset \boldsymbol{Q}$；设K的特征是$p>0$，则$K\supset \boldsymbol{Z}_p$。

证明 见上面的讨论。▌

每一个域K都可以看成某个素域的扩域。当域K的特征是$p>0$时，域K的许多性质都与常见的$\boldsymbol{Q},\boldsymbol{R},\boldsymbol{C}$的性质不同。例如任取$\alpha,\beta\in K$，我们有

$$(\alpha+\beta)^p=\alpha^p+\binom{p}{1}\alpha^{p-1}\beta+\cdots+\binom{p}{i}\alpha^{p-i}\beta^i+\cdots+\beta^p,$$

由于

$$p\left|\binom{p}{i}\right.,\quad i\neq 0,p,$$

$$p\times\gamma=p\times 1\times\gamma=0\times\gamma=0,\quad \forall\gamma\in K,$$

于是得出

$$(\alpha+\beta)^p=\alpha^p+\beta^p,$$

$$(\alpha-\beta)^p=\alpha^p+(-\beta)^p=\alpha^p+(-1)^p\beta^p=\alpha^p-\beta^p.$$

在上式中，如果$p\neq 2$，自然有$(-1)^p=-1$。如果$p=2$，也有$(-1)^p=1=1-(1+1)=-1$。又有

$$(\alpha\beta)^p=\alpha^p\beta^p,\quad (\beta^{-1})^p=(\beta^p)^{-1},$$

于是，在特征是$p>0$的域K中，映射

$$\rho:\ K\to K,$$

$$\rho(\gamma)=\gamma^p$$

是一个环单射。如果K是有限域时，单射即满射，所以ρ是K的自同构。

定义5.7 设K的特征是$p>0$。则映射ρ：$K\to K$，使$\rho(\gamma)=\gamma^p$，$\forall\gamma\in K$，称为K的**基本环单射**，或K的 Frobinius **映射**。当K为有限域时，基本环单射ρ又称为**基本自同构**。

如果在单位圆上，取一内接正多边形，且使1为此正多边形的一个顶点(参见例3)，则不难看出此正多边形的顶点所对应的复数对$\boldsymbol{C}$的乘法而言，构成一个有限的交换群。一般言之，我

们有下列的定理。

定理5.12 设G是域K的有限乘法子群，则G是一循环群。

证明 G显然是一个交换群。根据“有限生成的交换群的基本定理”的推论，即定理4.17的系，我们仅须证明G的初等因子$\{p_1^{s_1},\cdots,p_q^{s_q}\}$中的诸$p_i$皆不相同。假设$p_1=p_2$，则$G$中有两个子群$H_1,H_2$，使

$$o(H_1)=p_1^{s_1},\quad o(H_2)=p_1^{s_2},\quad H_1\cap H_2=\{1\}.$$

于是不妨设$s_1\leqslant s_2$，则下列方程式

$$x^{p_1^{s_2}}=1$$

在$G\subset K$中最少有$(p_1^{s_1}+p_1^{s_2}-1)$个不同的根。这在域K中是不可能的事。于是p_i皆不相同。所以G是循环群。▎

定理5.13 设K是有限域，其特征是$p>0$，$[K:\boldsymbol{Z}_p]=n$。则

$$K^*=K\setminus\{0\}=\{\gamma:\ \gamma\in K,\ \gamma\neq0\}$$

是一循环群．K的基数为p^n，K^*的基数为p^n-1。K中任意元素γ皆适合方程式

$$x^{p^n}-x=0.$$

K的基本自同构的阶是n。

证明 K^*显然是K的有限乘法子群，于是K^*是一个循环群。在$\boldsymbol{Z}_p$向量空间K中任取一组基$\{\alpha_1,\cdots,\alpha_n\}$，由此得出一坐标系

$$K\approx(\boldsymbol{Z}_p)^n.$$

显然$(\boldsymbol{Z}_p)^n$的基数是p^n，所以K的基数是p^n，以及K^*的基数是p^n-1。于是，乘法群K^*的阶数是p^n-1。所以我们有

$$\gamma^{p^n-1}=1,\quad \forall\gamma\in K^*.$$

由此立得K的任意元素都适合

$$x^{p^n}-x=0.$$

上式也可以理解成

$$\rho^n(\gamma)=\rho^{n-1}(\gamma^p)=\cdots=\gamma^{p^n}=\gamma,\qquad \forall\gamma\in K.$$

于是 ρ^n 是恒等映射。现设 ρ^m 为恒等映射。假若 $m<n$，则必有

$$\gamma^{p^m}=\rho^m(\gamma)=\gamma,\qquad \forall\gamma\in K,$$

即K的任意元素都适合

$$x^{p^m}-x=0.$$

而上式在域K中最多只有 p^m个根，所以K的所有元素又不可能都适合这个方程式。这个矛盾说明了 $m\geqslant n$。故 ρ 的阶是 n。▌

系(费马定理) 设 p 为一素数，$p\nmid a$，则有

$$a^{p-1}\equiv 1(\mathrm{mod}\ p).$$

(请对照定理1.8。)

上面这个定理，说明了基数是 p^n的有限域K的任意元素 γ 必然适合同一个方程式。反过来，我们也可以用这个方程式，来证明基数是任意给定的p^n的有限域K的存在性及唯一性。

定理5.14 设Ω是Z_p 的一个代数闭包。令 F_n 为下面的方程式在 Ω中的解的集合：

$$x^{p^n}-x=0,$$

则有

1) F_n是基数为p^n的有限域；
2) F_n是Ω中唯一的基数为p^n的有限域；
3) $F_n\subset F_m\Longleftrightarrow n|m$；
4) 设$F_n\subset F_m$，ρ为基本自同构，则ρ^n是F_m的阶为

$$m/n=[F_m:F_n]$$

的F_n自同构(所谓F_m的F_n自同构，即是F_m的自同构，且在F_n 上的作用为恒等映射)。

证明 1) 设$\alpha,\beta\in F_n$，即α,β适合方程$x^{p^n}-x=0$。故

$$\alpha^{p^n}=\alpha, \qquad \beta^{p^n}=\beta.$$

立得（参见定理5.11后面的论述）

$$(\alpha\pm\beta)^{p^n}=\alpha^{p^n}\pm\beta^{p^n}=\alpha\pm\beta, \qquad (\alpha\beta)^{p^n}=\alpha^{p^n}\beta^{p^n}=\alpha\beta,$$

$$(\beta^{-1})^{p^n}=(\beta^{p^n})^{-1}=\beta^{-1} \quad (\beta\neq 0).$$

即$\alpha\pm\beta,\alpha\beta$ 及 $\beta^{-1}(\beta\neq 0)$皆适合方程式 $x^{p^n}-x=0$，也即它们都属于 F_n。故 F_n 是一个域。

我们要证明$x^{p^n}-x$没有重根。因为$x^{p^n}-x$的重根必然也是它的导函数的根。而$x^{p^n}-x$的导函数$p^nx^{p^n-1}-1(=-1)$无根，所以$x^{p^n}-x$没有重根。于是 F_n 的基数是 p^n。

2）根据上一定理，基数为p^n的有限域是方程式$x^{p^n}-x=0$的解的集合，于是，F_n是Ω中唯一的基数为p^n的子域。

3）如果 $F_n\subset F_m$，设$[F_m:F_n]=l$，则 F_m是 l 维 F_n 向量空间。于是

$$p^m=(p^n)^l=p^{nl},$$

故 $m=nl$。反之，若$m=nl$，则显然有

$$\begin{aligned}x^{p^m}-x&=x(x^{p^m-1}-1)\\&=x(x^{p^n-1}-1)(x^{(p^m-1)/(p^n-1)}+\cdots+1),\end{aligned}$$

也即
$$x^{p^n}-x\mid x^{p^m}-x.$$

于是$x^{p^n}-x$ 的根都是 $x^{p^m}-x$ 的根，即 $F_n\subset F_m$。

4）ρ在F_m上的阶是m，所以ρ^n在F_m上的阶是 m/n。ρ 在 F_m 上的阶是 n，所以 ρ^n在 F_n 上是恒等映射。▎

讨论　在以后的“伽罗瓦理论”中，我们将看到F_m 的F_n 自同构仅有 $\rho^{ni}(i=0,1,\cdots,(m/n)-1)$这 n 个。

例 7　以上关于有限域的讨论，也可以应用到特征 0 的域上。我们举有关复数域 C的例子。

在复数域 $\boldsymbol{C}$ 中，下列方程式的根称为 n 次**单位根**：

$$x^n-1=0.$$

例如，一次单位根是 1，二次单位根是 ± 1，n 次单位根是

$$e^{2k\pi i/n},\quad k=0,1,\cdots,n-1.$$

连接 n 次单位根在复平面上对应的点，就得到单位圆的内接正 n 边形。

设 $\zeta\in\boldsymbol{C}$ 是 n 次单位根，而且对所有小于 n 的正整数 m，都有 $\zeta^m\neq 1$，则称 ζ 是 n 次**本原单位根**。例如在四次单位根的集合 $\{1,i,-1,-i\}$ 中，i 和 $-$i 是四次本原单位根，-1是二次本原单位根，1 是一次本原单位根。

不难看出，n 次单位根的集合

$$\{e^{2k\pi i/n}:\ k=0,1,\cdots,n-1\}$$

是一个 n 阶乘法循环群。n 次本原单位根即是此群的生成元。加法循环群 $\boldsymbol{Z}/n\boldsymbol{Z}$ 的元素$[m]$是生成元的充要条件是：存在 l，使

$$l[m]=[m]+[m]+\cdots+[m]=[lm]=[1],$$

也即$[m]$的主余数m_0与 n 互素。于是$\boldsymbol{Z}/n\boldsymbol{Z}$的生成元集合的基数是尤拉函数 $\varphi(n)$。由此，n 次本原单位根的个数也是 $\varphi(n)$。

设 ζ 是 n 次本原单位根，$f(x)$是 ζ 对$\boldsymbol{Q}$的极小多项式。我们要证明：

1） $f(x)\in\boldsymbol{Z}[x]$；

2） $f(x)$的根的集合是 n 次本原单位根的集合；

3） $\deg f(x)=\varphi(n)$。

证法如下。(请注意，n 为素数 p 时，例 3 已经证明了上面的三点。)

根据高斯引理及定理3.12，x^n-1在$\boldsymbol{Z}[x]$中的不可约因子都是本原多项式，而且在$\boldsymbol{Q}[x]$中也都不可约。显然，$x^n-1\in(f(x))$，于是$f(x)$必为 $\boldsymbol{Z}[x]$中的一个不可约的本原多项式。故 1)得证。

设 η 是 $f(x)$在$\boldsymbol{C}$中的一个根。我们恒有

$$\boldsymbol{Q}[\zeta]\approx\boldsymbol{Q}[x]/(f(x))\approx\boldsymbol{Q}[\eta],$$

$$\zeta^m=1 \iff \eta^m=1.$$

由于ζ是n次本原单位根，故η必为n次本原单位根。

我们要证明，如果η是n次本原单位根，则η必是$f(x)$的根。如此，则2)得证。设$\eta=\zeta^l$，必有$(l,n)=1$。令p为素数，$p|l$，我们来证明ζ^p是$f(x)$的根。如果这点得证，由于$\eta=(\zeta^p)^{l/p}$，于是以ζ^p代替ζ逐步归纳，即可证明η是$f(x)$的根。请注意，此时有$(p,n)=1$，即$p\nmid n$。令

$$\text{(1)} \qquad x^n-1=f(x)h(x), \qquad h(x)\in \boldsymbol{Z}[x].$$

如果ζ^p不是$f(x)$的根，则必是$h(x)$的根。于是ζ是$h(x^p)$的根。故有$f(x)|h(x^p)$。令σ为自然映射：

$$\sigma: \boldsymbol{Z}[x] \to (\boldsymbol{Z}/(p))[x],$$

则(1)式可以在映射σ下写成

$$\text{(2)} \qquad x^n-1=\sigma(f(x))\sigma(h(x))=\bar{f}(x)\bar{h}(x).$$

$f(x)|h(x^p)$可以写成

$$\bar{f}(x)|\bar{h}(x^p)=\bar{h}(x)^p$$

（此式中应用了$\boldsymbol{Z}_p$的基本自同构的性质）。于是在$\boldsymbol{Z}_p$的一个代数闭包Ω中$\bar{f}(x)$与$\bar{h}(x)$有共同的根。由(2)式即知x^n-1在Ω中有重根。然而x^n-1的导数是nx^{n-1}，但$n\neq 0$（因为$p\nmid n$），所以nx^{n-1}的根只有0，而0又显然不是x^n-1的根，于是x^n-1又无重根。这是一个矛盾。因此ζ^p必为$f(x)$的根。综上所述，我们证明了所有n次本原单位根都是$f(x)$的根。这就证明了2)。

因为x^n-1在$\boldsymbol{C}$中无重根，所以$f(x)$也无重根。根据2)，$\deg f(x)$等于n次本原单位根集合的基数，即$\varphi(n)$。因此3)得证。

根据以上证明的三点，我们定义n次**割圆多项式**（或称**分圆多项式**）$\varphi_n(x)$为上面的$f(x)$。

设η是n次单位根，即$\eta^n=1$。又令m是使得$\eta^m=1$的最小的正整数，则η是m次本原单位根。显然，根据群论，m是η的阶，于是有$m|n$。又从上面的2)，我们知道η是$\varphi_m(x)$的根，

于是立得

$$x^n - 1 = \prod_{m \mid n} \varphi_m(x).$$

考虑此式左右两侧的次数，我们得到下面这个常见的尤拉函数 $\varphi(n)$的公式

$$\varphi(n) = \sum_{m \mid n} \varphi(m).$$

例 8 设素数$p>2$。能不能用圆规直尺作出单位圆的内接正p^2边形呢？读者请参考例 4 及例 6。

根据上面的例 7，令ζ是p^2次本原单位根。易于看出

$$\varphi(p^2) = p(p-1).$$

于是$[Q[\zeta]:Q] = \varphi(p^2) = p(p-1)$，它有一个奇因子$p$，因此不可能存在一个二次扩域的链：

$$Q \subset K_1 \subset \cdots \subset K_n, \quad [K_1:Q] = 2, \quad [K_j:K_{j-1}] = 2,$$

使$\zeta \in K_n$。于是我们得知不可能用圆规直尺作出单位圆的内接正p^2边形。

与例 6 的结果相结合，我们证明了能用圆规直尺作出单位圆的内接正n边形的必要条件是

$$n = p_1 p_2 \cdots p_s \times 2^m,$$

其中$p_1, p_2, \cdots, p_s$是互异的费马素数。以后我们将证明这也是充分条件。

从上面的讨论，我们很容易导出，任给一个素数$p>2$，必然存在一个可以用圆规直尺作出的角，它不能用圆规直尺p等分（参考例 5）：如果单位圆的内接正p边形不能作出，则360°不能用圆规直尺p等分；如果能作出单位圆的内接正p边形，则其相邻的二顶点对原点的张角360°/p可以作出，但这个角不能再p等分了，否则就可以作出正p^2边形了。

习　题

1. 设有限域k有q个元素。问$k[x]$中有多少不可约的首1

二次多项式？

2. 在环Z[i]内，证明素理想(1+i)，(3)，(2+i)的商环Z[i]/(1+i)，Z[i]/(3)，Z[i]/(2+i)都是有限域，并求它们的特征。

3. 设K是有p^n(p为素数)个元素的域，证明：

(1) 若$(r,p^n-1)=(1)$，则在K内每个元素都可开r次方。

(2) 若$r|(p^n-1)$，则$a\in K$在K内可开r次方的充要条件是

$$a^{(p^n-1)/r}=1.$$

4. 设K是$\boldsymbol{Z}/3\boldsymbol{Z}=\boldsymbol{F}_3$的二次扩域，证明$\boldsymbol{F}_3$上多项式$x^8-1$在$K$内有一个本原根$\alpha$(即$x^8-1$的其它根都可表成$\alpha$的方幂)，并求$\alpha$在$\boldsymbol{F}_3$上的极小多项式。

5. 设$\boldsymbol{F}_p=\boldsymbol{Z}/p\boldsymbol{Z}$，$a$是$\boldsymbol{F}_p[x]$中一个$m$次不可约多项式$f(x)$在$\boldsymbol{F}_p$的$n$次扩域$K$内的一个根，证明$f(x)$的全部根是

$$a^p,\quad a^{p^2},\quad \cdots,\quad a^{p^m}=a.$$

6. 证明：对任一素数p及正整数m，都存在$\boldsymbol{F}_p$上的m次不可约多项式。

7. 设K,L分别是$\boldsymbol{F}_p$的m次和n次扩域，问m,n满足什么条件时，$K\cap L=\boldsymbol{F}_p$？(注：这里把K,L都看作$\boldsymbol{F}_p$的代数闭包的子域。)

8. 证明：$\boldsymbol{Q}(e^{2\pi i/(2k+1)})=\boldsymbol{Q}(e^{\pi i/(2k+1)})$。

9. 设p为素数，$K=\boldsymbol{Q}(e^{2\pi i/p})$，证明：

$$K\cap\boldsymbol{R}=\boldsymbol{Q}(e^{2\pi i/p}+e^{-2\pi i/p}).$$

§5 可离代数扩域

设K是域，L是K的扩域，$\alpha\in L$是对K的代数元，$f(x)\in K[x]$是α的极小多项式。在上文中，我们已看到，许多对扩域$K[\alpha]$的讨论可以归结为对多项式$f(x)$的研究。当K是$\boldsymbol{Q},\boldsymbol{R}$时，

$f(x)$皆无重根(详见下面的讨论)，然而当K的特征$p>0$时，$f(x)$可能有重根，由此产生出许多微妙的差异。我们要引入一些定义来阐明这个现象。

定义5.8 设K是域，L是K的扩域。令$g(x)\in K[x]$。如果$g(x)$在K的一个代数闭包Ω中没有重根，则称$g(x)$为**可离多项式**，又称为**可分多项式**。如果$\alpha\in L$是对K的代数元，而且其极小多项式$f(x)\in K[x]$是可离多项式，则称α是对K的**可离代数元**，又称为**可分代数元**。

一个多项式$g(x)$是不是可离多项式，可以用$g(x)$的导函数$g'(x)$检验出来。

我们有可离代数元的简单的判别条件如下：

引理1 设L是K的扩域，$\alpha\in L$。则α是对K的可离代数元$\Longleftrightarrow$ α是一个可离多项式$g(x)\in K[x]$的根。

证明 $\Longrightarrow$. 令$g(x)$为α对K的极小多项式即可。

$\Longleftarrow$. 设$f(x)$为α对K的极小多项式。于是

$$(f(x))=\{h(x):\ h(x)\in K[x],\ h(\alpha)=0\}\ni g(x),$$

即有$f(x)\mid g(x)$。由于$g(x)$无重根，所以$f(x)$无重根。▌

引理2 设L是K的扩域，$\alpha\in L$，α是对K的代数元。则α是对K的可离代数元$\Longleftrightarrow$ α的极小多项式$f(x)\in K[x]$的导函数$f'(x)\neq 0$。

证明 $\Longleftarrow$. 令Ω为$K[\alpha]$的一个代数闭包，则$f(x)$在$\Omega[x]$中可以完全分解。因为$f(x)$是$K[x]$中不可约多项式，所以$f(x)$是它在Ω中的任意根的极小多项式。由于$f'(x)\neq 0$，又有

$$\deg f'(x)<\deg f(x),$$

所以$f(x)$在Ω中的任一根α_i都不是$f'(x)$的根(否则与$f(x)$是α_i的极小多项式相矛盾)。于是$f'(x)$与$f(x)$没有公根。因此$f(x)$是一个可离多项式(参见定理3.20)。

$\Longrightarrow$. 设$f'(x)=0$。令$f(x)=(x-\alpha)h(x)$，其中$h(x)\in L[x]$。则有$f'(x)=(x-\alpha)h'(x)+h(x)$，故

$$0=f'(\alpha)=h(\alpha),$$

即 α 是 $f(x)$ 的重根。所以 $f(x)$ 不是一个可离多项式。 ▍

定义5.9 设 K 是域。如果 K 的任意扩域中的任意代数元都是可离代数元，则称 K 为**完全域**。

定理5.15 如果 K 的特征是0，或 K 是有限域，则 K 是完全域。

证明 如果 K 的特征是0，任取一个非常数的多项式

$$f(x)=a_0+a_1x+\cdots+a_nx^n,$$

则
$$f'(x)=a_1+\cdots+na_nx^{n-1}\neq 0,$$

故 K 是完全域。

如果 K 为有限域，设 α 是对 K 的代数元，则 $K[\alpha]$ 也是有限域。令 $K[\alpha]$ 的基数为 p^n，则 $K[\alpha]$ 的所有元素都是下面方程式的根(定理5.13)：

$$f(x)=x^{p^n}-x=0.$$

显然有 $f'(x)=p^nx^{p^n-1}-1=-1$，于是 $f(x)$ 与 $f'(x)$ 无公根，故 $f(x)$ 是一个可离多项式。按照引理1，α 是可离代数元。 ▍

例9 设 K 的特征是 $p>0$，$K[y]$ 是一元多项式环。$K(y)$ 为 $K[y]$ 的比域，即一元有理函数域。令 $\alpha=y^{1/p}$，则 α 适合下面的方程式：

$$f(x)=x^p-y=0.$$

因为 y 是 $K[y]$ 的素元，根据爱森斯坦判别定理，$f(x)\in K(y)[x]$ 是一个不可约多项式，也即是 α 的极小多项式。显然有

$$f'(x)=px^{p-1}=0,$$

所以 α 不是对 $K(y)$ 的可离代数元。如令 Ω 为 $K(y)$ 的一个代数闭包，则在 Ω 中

$$x^p-y=(x-\alpha)^p$$

只有一个根 α。 ▍

在一般的情形下，如果 K 不是完全域，则对 K 的代数元不一定是可离代数元。在这种情形下，可离代数元的加、减、乘、除

的结果是否还是可离代数元呢？答案是肯定的，详见下文。我们先引入下面的定义。

定义5.10 设 L 是 K 的扩域，如果 L 的元素都是对 K 的可离代数元，则称 L 是 K **的可离代数扩域**。

我们有下面的关于可离代数扩域的判别定理。

定理5.16 设域 K 的特征是 $p>0$，L 是 K 的有限扩域。令

$$KL^p=\left\{\sum_{i=1}^{n} a_i b_i^p:\ a_i\in K,\ b_i\in L\right\},$$

亦即由 L^p 生成的 K 向量空间。则有

1) KL^p 是 K 的有限扩域；

2) L 是 K 的可离代数扩域 $\Longleftrightarrow KL^p=L$。

证明 1) 任取 $\alpha,\beta\in KL^p\subset L$，不难看出，$K[\alpha,\beta]\subset KL^p$，所以 KL^p 是域。又有 $KL^p\subset L$，所以 KL^p 是 K 的有限扩域。

2) $\Longrightarrow$。任取 $\alpha\in L$。令 $f(x)$ 为 α 对 K 的极小多项式。我们自然有 $f(x)\in KL^p[x]$。因 $f(x)$ 无重根，根据引理1，α 也是对 KL^p 的可离代数元。令 α 对 KL^p 的极小多项式为 $g(x)\in KL^p[x]$，则 $g(x)$ 无重根。我们要证明 $\deg g(x)=1$。如此，则 $\alpha\in KL^p$。

因为 α 适合 $x^p-\alpha^p\in KL^p[x]$，所以有

$$g(x)\mid x^p-\alpha^p.$$

在 $L[x]$ 中考虑上式。其右侧是 $(x-\alpha)^p$，只有一个根。故 $g(x)$ 也只有一个根。但是 $g(x)$ 无重根，所以必有 $\deg g(x)=1$，也就是说 $\alpha\in KL^p$。

$\Longleftarrow$。我们任取 L 对 K 的一组基 $\{\gamma_j:\ j=1,2,\cdots,m\}$。显然，$KL^p$ 是由 $\{\gamma_j^p:\ j=1,2,\cdots,m\}$ 生成的 K 向量空间。因此，我们有

$$KL^p=L\Longleftrightarrow\{\gamma_j^p:\ j=1,2,\cdots,m\}\text{ 是 } L \text{ 的一组基}.$$

现在，我们任取 $\alpha\in L$。设 α 的代数次数是 n，则

$$\{\alpha^i:\ i=0,1,\cdots,n-1\}$$

对 K 是线性无关的。把它扩充成 L 的一组基

$$\{\alpha^i:\ i=0,1,\cdots,n-1\}\cup\{\beta_j:\ j=1,2,\cdots,m-n\}.$$

根据上面的讨论，我们知道

$$\{\alpha^{ip}:\ i=0,1,\cdots,n-1\}\cup\{\beta_j^p:\ j=1,2,\cdots,m-n\}$$

也是L的一组基，故$\{\alpha^{ip}:\ i=0,1,\cdots,n-1\}$对$K$是线性无关的。令$f(x)$为$\alpha$对$K$的极小多项式。假若$f(x)$不是可离多项式，则必有$f'(x)=0$，即

$$f'(x)=\left(\sum_{i=0}^{n}a_ix^i\right)'=\sum_{i=1}^{n}ia_ix^{i-1}=0.$$

也即 $$ia_i=0,\qquad \forall\, i=0,1,\cdots,n.$$

故 $$a_i\neq 0\implies p\mid i.$$

于是立得$f(x)\in K[x^p]$。因此$f(\alpha)=0$可以写成

$$\sum_{i=0}^{[n/p]}a_{ip}\alpha^{ip}=0,$$

这里$[n/p]$是n/p的整数部分。上式说明$\{\alpha^{ip}:\ i=0,1,\cdots,[n/p]\}$对$K$是线性相关的。这与前面导出的$\{\alpha^{ip}:\ i=0,1,\cdots,n-1\}$对$K$线性无关的事实相矛盾。于是$f(x)$必是可离多项式，即$\alpha$是可离代数元。▌

下面的两个定理，告诉我们可离代数扩域是很多的。

定理5.17 设L是K的扩域。如果$\alpha\in L$是对K的可离代数元，则$K[\alpha]$是K的可离代数扩域。

证明 只要对K的特征$p>0$的情形证明。根据上面的定理，我们仅须证明$K(K[\alpha])^p=K[\alpha]$。自然，我们只要证明$\alpha\in K(K[\alpha])^p$就足够了。与上定理证明中2)的"$\Longrightarrow$"部分完全一样，令$f(x)$是α对K的极小多项式，$g(x)$是α对$K(K[\alpha])^p$的极小多项式。因$f(x)\in K(K[\alpha])^p[x]$无重根，故$g(x)$也无重根。另一方面$\alpha$适合$x^p-\alpha^p\in K(K[\alpha])^p[x]$，所以必有

$$g(x)\mid x^p-\alpha^p.$$

在$L[x]$中考虑上式，立得$g(x)$只有一个根，而且不是重根。所以$\deg g(x)=1$，也即$\alpha\in K(K[\alpha])^p$。▌

定理5.18 设K的特征$p>0$，L是K的扩域，$\alpha\in L$是对K的代数元，$f(x)$是α对K的极小多项式。又设

$$f(x)\in K[x^{p^l}],\qquad f(x)\notin K[x^{p^{l+1}}]\quad (l\geq 0),$$

则$\beta=\alpha^{p^l}$是对K的可离代数元，β的代数次数是$\deg f(x)/p^l$，且$[K[\alpha]:K[\beta]]=p^l$。

证明 令$f(x)=g(x^{p^l})$。则显然有

$$g(\beta)=0,\qquad \deg g(x)=\deg f(x)/p^l.$$

于是

(1) $$[K[\beta]:K]\leqslant\deg f(x)/p^l.$$

显然，α适合$x^{p^l}-\beta\in K[\beta][x]$，于是

(2) $$[K[\alpha]:K[\beta]]\leqslant p^l.$$

根据定理5.6，我们又有

(3) $$\deg f(x)=[K[\alpha]:K]=[K[\alpha]:K[\beta]][K[\beta]:K].$$

由(1),(2),(3)式易于看出，(1),(2)二式中的等号必然成立，即β的代数次数是$\deg f(x)/p^l$，且

$$[K[\alpha]:K[\beta]]=p^l.$$

下面再证β是对K的可离代数元。由于$g(\beta)=0$，且

$$\deg g(x)=\deg f(x)/p^l=[K[\beta]:K],$$

故$g(x)$是β对K的极小多项式。又显然有$g(x)\notin K[x^p]$，所以

$$g'(x)\neq 0.$$

根据引理2，β是对K的可离代数元。▌

与定理5.6很类似的，我们有下述定理。

定理5.19 设L是S的有限可离代数扩域，S是K的有限可离代数扩域。则L是K的有限可离代数扩域。

证明 根据定理5.6，L自然是K的有限代数扩域。设K的特征$p>0$，不难看出下列等式（参见定理5.16）成立：

$$KL^p=K(SL)^p=KS^pL^p=SL^p=L,$$

于是L是K的有限可离代数扩域。▌

与K在L中的代数闭包相类似的，我们有K在L中的"可离代数闭包"的概念，见下定理。

定理5.20 设L是K的扩域，K的特征$p>0$。令

$$K_L^s=\{\alpha\in L:\ \alpha\text{是对}K\text{的可离代数元}\},$$

则K_L^s是域，称为K在L中的**可离代数闭包**。K_L^s有如下的性质：

1) 如果$\alpha\in L$是对K的代数元，则α对K_L^s的代数次数是形如p^l的正整数，$\alpha^{p^l}\in K_L^s$。此处l自然可能是0；

2) 如果$S\subset L$是K_L^s的有限扩域，则$[S:K_L^s]=p^l$。

证明 设$\alpha,\beta\in K_L^s$，则α,β自然是对K的代数元。我们仅须证明$K[\alpha,\beta]\subset K_L^s$。如此，则$K_L^s$的任意二元素$\alpha,\beta$加、减、乘、除的结果皆在$K_L^s$中，所以$K_L^s$是域。

显然，$K[\alpha],K[\beta]$皆是K的可离代数扩域。因此β适合一个可离多项式$f(x)\in K[x]\subset K[\alpha][x]$，所以$\beta$对$K[\alpha]$是可离代数元，于是$K[\alpha][\beta]$是$K[\alpha]$的可离代数扩张。根据定理5.19，$K[\alpha,\beta]$是$K$的可离代数扩域。于是$K[\alpha,\beta]\subset K_L^s$。这就证明了$K_L^s$是域。

现证明K_L^s的性质1)。α是对K_L^s的代数元，象在定理5.18中那样取l及$\beta=\alpha^{p^l}$，则β是对K_L^s的可离代数元。设其极小多项式为$g(x)\in K_L^s[x]$，

$$g(x)=\sum_{i=0}^{n}a_ix^i.$$

则立得β是对$K[a_0,a_1,\cdots,a_n]$的可离代数元。应用定理5.17及定理5.19，即知β是对K的可离代数元。于是有$\beta\in K_L^s$。定理5.18的结论告诉我们$[K_L^s[\alpha]:K_L^s]=p^l$。

再证明2)。设$S=K_L^s[\alpha_1,\cdots,\alpha_n]$。令$K_i=K_L^s[\alpha_1,\cdots,\alpha_i]$ $(i=1,2,\cdots,n)$。根据定理5.6，我们有

$$[S:K_L^s]=\prod_{i=0}^{n-1}[K_{i+1}:K_i],$$

其中$K_0=K_L^s$。自然，我们能证明$[K_{i+1}:K_i]=p^r$便足够了。根据

1)，我们知道存在非负整数 m，使

$$\alpha_{i+1}^{p^m} \in K_0 \subset K_i.$$

令 $g(x)$ 为 α_{i+1} 对 K_i 的极小多项式。又设 $g(x) \in K_i[x^{p^r}]$，但

$$g(x) \notin K_i[x^{p^{r+1}}].$$

再令 $\beta = \alpha_{i+1}^{p^r}$ 以及 $g(x) = h(x^{p^r})$。根据定理5.18，则知 β 是对 K_i 的可离代数元，$h(x)$ 无重根。显然

$$g(x) \mid (x^{p^m} - \alpha_{i+1}^{p^m}),$$

故
$$h(x) \mid (x^{p^{m-r}} - (\alpha_{i+1}^{p^r})^{p^{m-r}}) \in K_i[x].$$

而上式右侧只有一个根，故 $h(x)$ 只有一个根，而且不是重根。因此 $\deg h(x) = 1$，即 $\beta \in K_i$。由定理5.8，就有

$$[K_{i+1}:K_i] = [K_{i+1}:K_i[\beta]] = p^r. \quad \blacksquare$$

我们把以上定理中应用的一个概念，用下面的定义显示出来。

定义5.11 设 L 是 K 的扩域，K 的特征为 $p>0$，$\alpha \in L$。如果存在非负整数 l，使 $\alpha^{p^l} \in K$，则称 α 是对 K 的**纯不可离元**。如果 L 的所有元素都是对 K 的纯不可离元，则称 L 是 K 的**纯不可离代数扩域**。

应用纯不可离的概念，定理5.20可以理解为：如果 L 是 K 的代数扩域，则存在 K 在 L 中的可离代数闭包 K_L^s，使

1) K_L^s 是 K 的可离代数扩张；

2) L 是 K_L^s 的纯不可离代数扩域。

下面这个定理，使有限可离代数扩域的构造简单易懂。因为特征零的域都是完全域，所以也都适合下面的定理。

定理5.21 设 L 是 K 的有限可离代数扩域，则 L 是 K 的**单扩域**，即存在 $\alpha \in L$，使 $L = K[\alpha]$。

证明 设 L 是 K 的有限可离代数扩域，所以存在 $\alpha_1, \alpha_2, \cdots, \alpha_n \in L$，使

$$L = K[\alpha_1, \alpha_2, \cdots, \alpha_n].$$

显然，我们仅须证明：如果 α，β 是对 K 的可离代数元，则

$$K[\alpha, \beta] = K[\gamma],$$

其中 $\gamma \in K[\alpha,\beta]$。

如果K为有限域，$K[\alpha,\beta]$自然是有限域。根据定理5.13，$K[\alpha,\beta]^*$是一个循环群。令γ为其一个生成元，则自然有

$$K[\alpha,\beta]=K[\gamma].$$

现在我们仅须考虑K是无限域的情形。令Ω为$K[\alpha,\beta]$的一个代数闭包，$f(x)\in K[x]$为α的极小多项式，$g(x)\in K[x]$为β的极小多项式。令$f(x),g(x)$在$\Omega[x]$中分解如下：

$$f(x)=\prod_{i=1}^{n}(x-\alpha_i),\quad \alpha_1=\alpha,$$

$$g(x)=\prod_{j=1}^{m}(x-\beta_j),\quad \beta_1=\beta.$$

显然，$f(x),g(x)$皆无重根。在K中取一个$c\neq 0$，使

$$(*)\qquad c\neq -\frac{\alpha_1-\alpha_i}{\beta_1-\beta_j},\qquad \forall i=2,\cdots,n,\ j=2,\cdots,m.$$

因为K是无限集，所以这样的c是存在的。令

$$\gamma=\alpha_1+c\beta_1=\alpha+c\beta,$$

则显然有$K[\alpha,\beta]\supset K[\gamma]$。我们将证明$\beta=\beta_1\in K[\gamma]$。如此，则自然导出$\alpha=\gamma-c\beta\in K[\gamma]$，即有$K[\alpha,\beta]=K[\gamma]$。

β适合$K[\gamma][x]$中的两个多项式$g(x)$及$f(\gamma-cx)$，于是β对$K[\gamma]$的极小多项式$h(x)$必然是$g(x)$与$f(\gamma-cx)$的一个公因元。我们在$\Omega[x]$中考虑$g(x)$与$f(\gamma-cx)$的公因元。$g(x)$的因元皆形如$x-\beta_j(j=1,2,\cdots,m)$。由$(*)$式容易看出，如果$\gamma=\alpha_i+c\beta_j$，则必有$i=j=1$。所以当$j>1$时，

$$\gamma-c\beta_j\neq\alpha_i\quad(\forall i=1,2,\cdots,n).$$

所以此时$f(\gamma-c\beta_j)\neq 0$，也即$x-\beta_j$不是$f(\gamma-cx)$的因元($j>1$)。于是$g(x)$与$f(\gamma-cx)$在$\Omega[x]$中的最大公因元是$x-\beta_1=x-\beta$。自然，$g(x)$与$f(\gamma-cx)$在$K[\gamma][x]$中的公因元$h(x)$也只能是$x-\beta$。这样，我们导出了$\beta\in K[\gamma]$。▌

例10 我们举一个不是单扩域的例子。取两个变数符号x，

y。令 $\boldsymbol{Z}_p(x,y)$ 为二元有理函数域。

$$\boldsymbol{Z}_p(x^p,y^p)\subset\boldsymbol{Z}_p(x,y).$$

参照例 9，不难看出，x,y 都是对 $\boldsymbol{Z}_p(x^p,y^p)$ 的 p 次代数元，而且有

$$[\boldsymbol{Z}_p(x,y):\boldsymbol{Z}_p(x^p,y^p)]=p^2.$$

任取 $\gamma\in\boldsymbol{Z}_p(x,y)$，读者自证

$$\gamma^p\in\boldsymbol{Z}_p(x^p,y^p).$$

于是有

$$[\boldsymbol{Z}_p(x^p,y^p)[\gamma]:\boldsymbol{Z}_p(x^p,y^p)]\leqslant p,$$

故 $$\boldsymbol{Z}_p(x,y)=\boldsymbol{Z}_p(x^p,y^p)[x,y]\neq\boldsymbol{Z}_p(x^p,y^p)[\gamma].$$

习　题

1. 设 $\omega=e^{2\pi i/7}$，对每一个中间域 K，$\boldsymbol{Q}\subset K\subset\boldsymbol{Q}(\omega)$，求一生成元 β，使 $K=\boldsymbol{Q}(\beta)$。

2. 设 L 是 K 的有限扩域，已知对每一个 $w\in L$，存在 $f(x)\in K[x]$，使 $f(w)=0$，但 $f'(w)\neq 0$。证明存在 $v\in L$，使 $L=K(v)$。

3. 设 L 是 K 的有限扩域。证明：$L=K(v)\Longleftrightarrow L$ 与 K 之间，只有有限多个中间域。

4. 找出 v，使 $\boldsymbol{Q}(\sqrt{2},\sqrt{3})=\boldsymbol{Q}(v)$。

5. 令 $\boldsymbol{F}_p=\boldsymbol{Z}/p\boldsymbol{Z}$（$p$ 为素数），x 是变量。又令 $\boldsymbol{F}_p[x]$ 上多项式 y^p-x 的一个零点为 a，证明 $\boldsymbol{F}_p(a)$ 在 $\boldsymbol{F}_p(x)$ 上不可离。

6. 设 K 是特征为 p 的域，若 $\beta=a^{p^l}\in K$，但 $a^{p^{l-1}}\notin K$。证明 $x^{p^l}-\beta$ 在 $K[x]$ 内不可约，从而 a 在 K 上为不可离代数元。

7. 证明完全域的任一代数扩域仍是完全域。

8. 设 K 是特征为 p 的域，L 是 K 的扩域。如果 $a\in L$，a 对域 $K(a^p)$ 是可离代数元，证明 $a\in K(a^p)$。

9. 设 K 是特征为 p 的域，证明 K 是完全域的充要条件是：

K内每个元素在K内可开p次方。

10．设$f(x)$是域K上的不可约多项式，证明$f(x)$的所有零点都有相同的重数。

11．设K是特征为p的域，$p|n$。证明在K内不存在n个不同的n次单位根。

12．设L是K的扩域，$\alpha\in L$对K是纯不可离的，那么α对任一中间子域F也是纯不可离的。

13．设$K\subset F\subset L$，L对F纯不可离，F对K也纯不可离。证明L对K纯不可离。

14．设L是K的扩域，$\alpha\in L$在K上可离，$\beta\in L$对K纯不可离，证明$K(\alpha,\beta)=K(\alpha+\beta)$，又若$\alpha\neq 0$，$\beta\neq 0$，则

$$K(\alpha,\beta)=K(\alpha\beta).$$

15．设域K特征$p>0$，L是K的n次扩域，$p\nmid n$。证明L对K是可离的。

16．设域K特征$p>0$，L是K的扩域。证明$\alpha\in L$在K上可离的充要条件是：对一切正整数n，$K(\alpha)=K(\alpha^{p^n})$。

17．设域K特征$p>0$，$L=K(\alpha,\beta)$，且$\alpha^p,\beta^p\in K$，$[L:K]=p^2$。证明L不是K的单扩张。

§6 伽罗瓦理论

本节的中心旨趣是一个域L的变换群G。读者可以参看第二章§2“集合上的变换群”。我们先引入下面的概念。

定义5.12 设Ω是K的代数闭包，$f(x)\in K[x]$是一个非常数的多项式。在$\Omega[x]$中$f(x)$分解如下：

$$f(x)=a_0\prod_{i=1}^{n}(x-\alpha_i),$$

则$K[\alpha_1,\cdots,\alpha_n]$称为$f(x)$对$K$的**分裂域**，或简称为$f(x)$的**分裂域**。

定义5.13 设L是K的代数扩域。如果对于$K[x]$中任意一个不可约的多项式$f(x)$，只要$f(x)$在L中有一个根，$f(x)$就可以在$L[x]$中分解成一次式的乘积，则称L是K的一个**正规扩域**。

例11 令Ω为K的代数闭包，则显然Ω是K的正规扩域。

设K为特征p的有限域，L是K的有限代数扩域。令L的基数为p^t。设$f(x)$为$K[x]$中一个不可约多项式，$\alpha\in L$是$f(x)$的一个根。我们知道，α是多项式

$$x^{p^t}-x\in K[x]$$

的根，于是，我们有

$$f(x)\mid x^{p^t}-x=\prod_{\beta\in L}(x-\beta)\in L[x].$$

所以$f(x)$在$L[x]$中可以分解成一次式的乘积。我们证明了L是K的正规扩域。

设$K=\mathbf{Q}$，$L=\mathbf{Q}[\sqrt[3]{3}]$。则$f(x)=x^3-3$是$\mathbf{Q}[x]$中的一个不可约多项式(爱森斯坦判别定理)，而且在$L$中有一个根$\sqrt[3]{3}$。然而其另外两个根

$$\sqrt[3]{3}\,e^{2\pi i/3},\qquad \sqrt[3]{3}\,e^{4\pi i/3}$$

不是实数，因此显然不在L中。所以$f(x)$在$L[x]$中不能分解成一次式的乘积，于是L不是$\mathbf{Q}$的正规扩域。▎

下面的定理给出了定义5.12及定义5.13这两个概念的联系。

定理5.22 域L是域K的有限正规扩域$\Longleftrightarrow$ L是某个非常数多项式的分裂域。

证明 $\Longrightarrow$。设$L=K[\alpha_1,\cdots,\alpha_n]$，$\alpha_i$对$K$的极小多项式是$f_i(x)(i=1,\cdots,n)$。根据正规扩域的定义，$f_i(x)$在$L[x]$中可以分解成一次式的乘积。于是不难看出，$L$即是下面的$f(x)$对$K$的分裂域：

$$f(x)=\prod_{i=1}^{n}f_i(x).$$

$\Longleftarrow$。设 $f(x)$ 在 $L[x]$ 中分解如下：

$$(1)\qquad f(x)=a_0\prod_{i=1}^{m}(x-\alpha_i)$$

$$=a_0(x^m-\theta_1x^{m-1}+\cdots+(-1)^i\theta_ix^{m-i}+\cdots+(-1)^m\theta_m).$$

任取一个不可约多项式 $g(x)\in K[x]$，设 β 为 $g(x)$ 在 L 中的一个根。因为 $L=K[\alpha_1,\cdots,\alpha_m]$，所以有

$$(2)\qquad \beta=\sum_{\text{有限}}a_{i_1\cdots i_m}\alpha_1^{i_1}\cdots\alpha_m^{i_m},$$

其中 $a_{i_1\cdots i_m}\in K$。令 S_m 为$\{1,2,\cdots,m\}$的对称群。任取 $\sigma\in S_m$，令 $\sigma(\beta)$定义如下：

$$(3)\qquad \sigma(\beta)=\sum a_{i_1\cdots i_m}\alpha_{\sigma(1)}^{i_1}\cdots\alpha_{\sigma(m)}^{i_m}\in L;$$

再令 $h(x)$定义如下：

$$(4)\qquad h(x)=\prod_{\sigma\in S_m}(x-\sigma(\beta))$$

$$=x^{m!}+\cdots+a_ix^{m!-i}+\cdots+a_{m!}.$$

请注意，在(1)式中的 θ_i是 $\alpha_1,\cdots,\alpha_m$的初等对称多项式，$\theta_i\in K$。在(4)式中的系数 a_i都是 $\alpha_1,\cdots,\alpha_m$的对称多项式。根据定理3.16，我们立得

$$a_i\in K[\theta_1,\cdots,\theta_m]=K,\qquad h(x)\in K[x].$$

于是 β 的极小多项式 $g(x)$必然适合下列关系：

$$g(x)\mid h(x).$$

但在 $L[x]$中，$h(x)$可以分解成一次式的乘积(见(4)式)，故$g(x)$在 $L[x]$中也可以分解成一次式的乘积。❙

下面的定义是本节的中心概念。

定义5.14 如果 L 是域 K 的有限的、可离的正规扩域，则称 L 是 K 的**伽罗瓦扩域**。

当 L 是 K 的伽罗瓦扩域时，极有意义的是 L 的 K 自同构群。

我们用下面的符号：设域S是域R的扩域，用$G(S/R)$表示S的R自同构群(称为S在R上的**伽罗瓦群**)，即

$$G(S/R)=\{\sigma:\ \sigma\text{ 是}S\text{ 的自同构，}\sigma\text{ 在}R\text{上的作用是恒等映射，即 }\sigma(r)=r,\ \forall r\in R\}.$$

设G是域S的一个自同构群，则用$F(G)$表示在G作用下S的不变元的集合，即

$$F(G)=\{s:\ s\in S,\ g(s)=s,\ \ \forall g\in G\}.$$

我们有如下的引理。

引理 设G是域S的一个自同构群，则$F(G)$恒为域，称为G的**不变域**。

证明 任取$g\in G$，则恒有

$$g(0)=0,\qquad g(1)=1,$$

所以$0,1\in F(G)$。设$\alpha,\beta\in F(G)$，则$\forall g\in G$，恒有

$$g(\alpha\pm\beta)=g(\alpha)\pm g(\beta)=\alpha\pm\beta,$$

$$g(\alpha\beta)=g(\alpha)g(\beta)=\alpha\beta.$$

所以$\alpha\pm\beta,\alpha\beta\in F(G)$。又当$\beta\neq 0$时，恒有

$$1=g(1)=g(\beta\beta^{-1})=g(\beta)g(\beta^{-1})=\beta g(\beta^{-1}),$$

所以

$$g(\beta^{-1})=\beta^{-1}.$$

于是$\beta^{-1}\in F(G)$。所以$F(G)$是域。▎

我们有下面的重要的定理。

定理5.23(伽罗瓦理论的基本定理) 设L是域K的伽罗瓦扩域，则我们恒有

1) 任意取一个中间域S：$L\supset S\supset K$，则L是S的伽罗瓦扩域，$o(G(L/S))=[L:S]$，且$G(L/S)$的不变域$F(G(L/S))=S$；

2) 任取$G(L/S)$的子群H，则

$$[L:F(H)]=o(H),\qquad G(L/F(H))=H;$$

3) S是K的正规扩域$\Longrightarrow G(L/S)$是$G(L/K)$的正规子群；H是$G(L/K)$的正规子群$\Longrightarrow F(H)$是K的正规扩域，在这种情形下，有

$$G(S, K) \approx G(L, K)/G(L/S).$$

证明 1) L 显然是 S 的有限可离代数扩域。又，L 是某一个多项式 $f(x) \subset K[x] \subset S[x]$ 的分裂域，所以 L 是 S 的正规扩域。因此，L 是 S 的伽罗瓦扩域。

按照定理5.21，L 是 S 的单扩域，$L = S[\alpha]$。设 α 的极小多项式为 $f(x)$。因为 $f(x)$ 在 L 中有一个根 α，L 是 S 的正规扩域，所以 $f(x)$ 在 $L[x]$ 中可以分解成下式：

$$f(x) = \prod_{i=1}^{n}(x - \alpha_i), \qquad \alpha_1 = \alpha.$$

α 又是对 S 的可离代数元，所以其极小多项式是可离多项式，因此所有的 α_i 皆不相同。

根据定理5.9，S 的恒等映射 id 可以扩张成由 $S[\alpha_1]$ 到 $S[\alpha_i]$ 的同构 σ_i，使

$$\sigma_i(\alpha_1) = \alpha_i, \qquad i = 1, 2, \cdots, n.$$

显然，我们有 $S[\alpha_i] \subset S[\alpha] = S[\alpha_1]$，且

$$\dim_S S[\alpha_1] = \deg f(x) = \dim_S S[\alpha_i].$$

如此立得 $L = S[\alpha] = S[\alpha_1] = S[\alpha_i]$。于是 σ_i 都是 L 的 S 自同构，且两两不同。故

$$o(G(L/S)) \geqslant n = [L:S].$$

任取 $\sigma \in G(L/S)$，则恒有

$$0 = \sigma(0) = \sigma(f(\alpha_1)) = f(\sigma(\alpha_1)).$$

于是 $\sigma(\alpha_1)$ 必为 $f(x)$ 的一个根，也即有某个 i，$1 \leqslant i \leqslant n$，使

$$\sigma(\alpha_1) = \alpha_i.$$

显然，L 的 S 自同构 σ 由上式唯一确定，所以必有

$$\sigma = \sigma_i.$$

故
$$o(G(L/S)) = n = [L:S].$$

现在我们要证明 $F(G(L/S)) = S$。仅须证明，任取 $\beta \notin S$，$\beta \in L$，必有一 $\sigma_i \in G(L/S)$，使 $\sigma_i(\beta) \neq \beta$ 便已足够了。

令 β 对 S 的极小多项式为 $g(x)$，其在 $L[x]$ 中的分解式为

$$g(x)=\prod_{j=1}^{m}(x-\beta_j),\qquad m>1,\ \beta_1=\beta.$$

令 $R_1=S[\beta_1]$，$R_2=S[\beta_2]$。根据定理5.9，S 的恒等映射 id 可扩张成同构 γ：$R_1(=S[\beta_1])\to R_2(=S[\beta_2])$，使

$$\gamma(\beta_1)=\beta_2\neq\beta_1.$$

令 α（请注意：$L=K[\alpha]=R_1[\alpha]=R_2[\alpha]$）对 R_1 的极小多项式为 $h(x)$。又设 Ω 是 L 的一个代数闭包，因此也是 R_2 的一个代数闭包。于是在 Ω 中，$\gamma(h(x))\in R_2[x]$ 有解。令其一解为 $\bar{\alpha}$。根据定理5.9，S 同构 γ 可以扩张成 $L(=R_1[\alpha])$ 到 $R_2[\bar{\alpha}]$ 的一个 S 同构 γ'，使

$$\gamma'(\alpha)=\bar{\alpha}.$$

然而，S 同构 γ' 也是一个 K 同构，故

$$0=f(\alpha)=\gamma'(f(\alpha))=f(\gamma'(\alpha)).$$

所以 $\gamma'(\alpha)$ 必等于上面的某个 α_i，也即 γ' 必为某个 $\sigma_i\in G(L/S)$。故

$$\sigma_i(\beta)=\gamma'(\beta_1)=\beta_2\neq\beta_1=\beta.$$

这就证明了 $F(G(L/S))=S$。

2）令 $S=F(H)$。显然 $H\subset G(L/S)$。所以根据 1)，我们得出

$$o(H)\leqslant o(G(L/S))=[L:S]=[L:F(H)].$$

设 $L=K[\alpha]$，$H=\{\gamma_1,\cdots,\gamma_m\}$。令

$$\prod_{i=1}^{m}(x-\gamma_i(\alpha))=x^m+b_1x^{m-1}+\cdots+b_m.$$

则显然可见，上式在 H 作用下是不变的，所以 $b_i\in S(\forall i)$，即

$$\prod_{i=1}^{m}(x-\gamma_i(\alpha))\in S[x].$$

所以
$$[L:F(H)]=[L:S]\leqslant m=o(H).$$

由上面两个不等式，我们有

$$[L:F(H)]=o(H),\qquad G(L/F(H))=H.$$

3) 设S是K的正规扩域，则显然S是K的伽罗瓦扩域。设$S=K[\beta]$，β对K的极小多项式为$g(x)$。$g(x)$在$S[x]$中可以分解成

$$g(x)=\prod_{j=1}^{m}(x-\beta_j),\qquad \beta_1=\beta.$$

任取$\sigma\in G(L/K)$，则显然有

$$0=g(\beta)=\sigma(g(\beta))=g(\sigma(\beta)).$$

于是$\sigma(\beta)$也是$g(x)$的根，所以$\sigma(\beta)\in S$，以及σ引生出S的一个K自同构$\bar{\sigma}$($\bar{\sigma}$由$\beta\mapsto\sigma(\beta)$所规定)。这样，

$$\pi:\ \sigma\mapsto\bar{\sigma}$$

定义了一个映射

$$\pi:\ G(L/K)\to G(S/K).$$

显然，π是一个群映射，而且$\ker(\pi)=G(L/S)$。所以$G(L/S)$是$G(L/K)$的一个正规子群。我们要证明π是一个满射。如此，则自然得出下面两个群的同构：

$$G(L/K)/G(L/S)\simeq G(S/K).$$

任取$\bar{\sigma}\in G(S/K)$。设$L=S[\alpha]$，α对S的极小多项式是$h(x)\in S[x]$。根据定理5.9，$\bar{\sigma}$可以扩张成$L(=S[\alpha])$到$S[\bar{\alpha}]$的一个同构σ，此处$\bar{\alpha}$是$\bar{\sigma}(h(x))\in S[x]$在$L$的一个代数闭包$\Omega$中的一个根。令$f(x)$为$\alpha$对$K$的极小多项式，则又有

$$0=\sigma(f(\alpha))=f(\sigma(\alpha))=f(\bar{\alpha}).$$

于是$\bar{\alpha}$是$f(x)$的一个根α_i。不难看出$S[\bar{\alpha}]=L$，$\sigma\in G(L/K)$，以及

$$\pi(\sigma)=\bar{\sigma}.$$

所以π是一个满射。

现设H是$G(L/K)$的一个正规子群。令$S=F(H)$，以及

$$G(L/K)=Hg_1\cup Hg_2\cup\cdots\cup Hg_l,$$

其中 $l=[G(L/K):H]$。设 $m=o(H)=[L:S]$，则 $ml=[L:K]=o(G(L/K))$。又设 $S=K[\beta]$。则有

$$\sigma g_i(\beta)=g_i\sigma'(\beta)=g_i(\beta),\qquad \forall \sigma\in H,\ i=1,\cdots,l,$$

式中 σ' 为 H 中某元素，满足 $\sigma g_i=g_i\sigma'$。从上式立得

$$g_i(\beta)\in S,\qquad \forall i=1,\cdots,l.$$

令

$$h(x)=\prod_{i=1}^{l}(x-g_i(\beta)),$$

其中有一个 g_i 可以取为恒等映射。易见 $h(x)$ 在 $g_j(j=1,\cdots,l)$ 作用下不变，所以在 $G(L/K)$ 作用下不变，故 $h(x)\in K[x]$。显然，S 是 $h(x)$ 的分裂域，于是 S 是 K 的正规扩域。 ▎

讨论 1）上面这个基本定理，可以理解成所有中间域 $\{S\}$ 与 $G(L/K)$ 的所有子群 $\{H\}$ 之间存在着一个自然的单满映射：S 对应到 $G(L/S)$，H 对应到 $F(H)$。在这个单满映射下，K 的正规扩域与 $G(L/K)$ 的正规子群自然地互相对应。

2）因为有限群 $G(L/K)$ 只有有限多个子群，所以伽罗瓦扩域 L 与 K 之间，只有有限多个中间域。

例12 我们实际计算一些例子。读者可能察觉到，在上面的证明中，我们曾几次用到了定理5.9。在下面的计算中我们也将应用定理5.9。

令 L 是下面的多项式对 $\mathbf{Q}$ 的分裂域：

$$f(x)=x^3-2.$$

令 $\zeta=e^{2\pi i/3}$。则显然，在 $\boldsymbol{C}$ 中上式分解成

$$x^3-2=(x-\sqrt[3]{2})(x-\sqrt[3]{2}\zeta)(x-\sqrt[3]{2}\zeta^2).$$

于是

$$L=\mathbf{Q}[\sqrt[3]{2},\ \sqrt[3]{2}\zeta,\ \sqrt[3]{2}\zeta^2]=\mathbf{Q}[\sqrt[3]{2},\zeta].$$

令 $S=\mathbf{Q}[\zeta]\subset L$。$\zeta$ 的极小多项式是三次割圆多项式

$$\varphi_3(x)=\frac{x^3-1}{x-1}=x^2+x+1=(x-\zeta)(x-\zeta^2).$$

于是有两个同构

$$\gamma_1:\ \mathbf{Q}[\zeta]\to\mathbf{Q}[\zeta],\qquad \gamma_1(\zeta)=\zeta,$$
$$\gamma_2:\ \mathbf{Q}[\zeta]\to\mathbf{Q}[\zeta^2](=\mathbf{Q}[\zeta]),\qquad \gamma_2(\zeta)=\zeta^2.$$

显然 $[\mathbf{Q}[\sqrt[3]{2}]:\mathbf{Q}]=3$。所以我们有

$$2,3\mid[\mathbf{Q}[\sqrt[3]{2},\zeta]:\mathbf{Q}]=[\mathbf{Q}[\sqrt[3]{2},\zeta]:\mathbf{Q}[\zeta]][\mathbf{Q}[\zeta]:\mathbf{Q}]\leqslant 6.$$

于是得出

$$[\mathbf{Q}[\sqrt[3]{2},\zeta]:\mathbf{Q}]=6,\qquad [\mathbf{Q}[\sqrt[3]{2},\zeta]:\mathbf{Q}[\zeta]]=3.$$

根据定理5.9，γ_1,γ_2都有三个不同的扩张：

$$\gamma_1:\begin{cases}\sigma_1:\ \sigma_1(\zeta)=\zeta, & \sigma_1(\sqrt[3]{2})=\sqrt[3]{2},\\ \sigma_2:\ \sigma_2(\zeta)=\zeta, & \sigma_2(\sqrt[3]{2})=\sqrt[3]{2}\zeta,\\ \sigma_3:\ \sigma_3(\zeta)=\zeta, & \sigma_3(\sqrt[3]{2})=\sqrt[3]{2}\zeta^2,\end{cases}$$

$$\gamma_2:\begin{cases}\sigma_4:\ \sigma_4(\zeta)=\zeta^2, & \sigma_4(\sqrt[3]{2})=\sqrt[3]{2},\\ \sigma_5:\ \sigma_5(\zeta)=\zeta^2, & \sigma_5(\sqrt[3]{2})=\sqrt[3]{2}\zeta,\\ \sigma_6:\ \sigma_6(\zeta)=\zeta^2, & \sigma_6(\sqrt[3]{2})=\sqrt[3]{2}\zeta^2.\end{cases}$$

上面的六个 σ_i 又可以看成 S_3的元素如下：令

$$a_1=\sqrt[3]{2},\qquad a_2=\sqrt[3]{2}\zeta,\qquad a_3=\sqrt[3]{2}\zeta^2.$$

则 σ_i显然是(a_1,a_2,a_3)的对称变换。读者不难看出

$$\sigma_1\leftrightarrow(1)(2)(3),\qquad \sigma_2\leftrightarrow(1,2,3),\qquad \sigma_3\leftrightarrow(1,3,2),$$
$$\sigma_4\leftrightarrow(1)(2,3),\qquad \sigma_5\leftrightarrow(1,2)(3),\qquad \sigma_6\leftrightarrow(1,3)(2).$$

一般言之，如果L是一个多项式$f(x)$在K的分裂域，则$G(L/K)$的元素都可以考虑成$f(x)$的n个根的对称变换。于是$G(L/K)$可以认同为S_n的一个子群，这里$n=\deg f(x)$。

例13　设K是一个基数为p^n的有限域，L是K的m次扩张。于是L的基数是p^{nm}。令ρ为基本映射，即

$$\rho(a)=a^p,\qquad \forall a\in L.$$

根据定理5.14，ρ^n是L的阶为m的K自同构。由例11中的讨论，L是K的伽罗瓦扩域。于是

$$o(G(L/K)) = [L:K] = m.$$

由此立得

$$G(L/K) = \{\rho^{0n}(=\mathrm{id}), \rho^n, \cdots, \rho^{(m-1)n}\},$$

即$G(L/K)$为由ρ^n生成的循环群。

例14 根据例6，设p为奇素数，则能用圆规直尺作出单位圆的内接正p边形$\Longrightarrow p$是一个费马素数，即

$$p = 2^{2^q} + 1.$$

现在我们可以证明，它也是充分条件。

令$\zeta = e^{2\pi i/p}$，即ζ是下面方程式的一个根：

$$\varphi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1 = 0.$$

显然，$\mathbf{Q}[\zeta]$是$x^p - 1$对$\mathbf{Q}$的分裂域。所以$\mathbf{Q}[\zeta]$是$\mathbf{Q}$的伽罗瓦扩域，以及(参见例3)

$$[\mathbf{Q}[\zeta]:\mathbf{Q}] = p - 1 = 2^{2^q}.$$

于是，我们有

$$o(G(\mathbf{Q}[\zeta]/\mathbf{Q})) = 2^{2^q}.$$

根据第二章§6，$G(\mathbf{Q}[\zeta]/\mathbf{Q})$是一个2群。应用定理2.14，存在一系列的子群$G_i$，使

$$G(\mathbf{Q}[\zeta]/\mathbf{Q}) = G_{2^{2^q}} \triangleright \cdots \triangleright G_i \triangleright G_{i-1} \triangleright \cdots \triangleright G_0 = \{e\}.$$

$$[G_i:G_{i-1}] = 2, \qquad \forall i = 1, 2, \cdots, 2^{2^q}.$$

应用伽罗瓦理论的基本定理，存在一系列的中间域K_i，使

$$\mathbf{Q} = K_{2^{2^q}} \subset \cdots \subset K_i \subset K_{i-1} \subset \cdots \subset K_0 = \mathbf{Q}[\zeta],$$

$$[K_{i-1}:K_i] = 2, \qquad \forall i = 1, 2, \cdots, 2^{2^q}.$$

应用例4的讨论所得出的圆规直尺作图的充要条件，我们得知，上面的一系列的中间域的存在，意味着正p边形可以作出。

在例 8 中，我们证明了能用圆规直尺作出单位圆的内接正 n 边形(此处$n>2$，不一定是素数)的必要条件是

$$n=p_1p_2\cdots p_s2^m,$$

其中$p_1,p_2,\cdots,p_s$是互异的费马素数.我们来证明这也是充分条件。

我们无非是要作出$2\pi/n$ 角。应用“部分分式”，有

$$\frac{2\pi}{n}=2\pi\cdot\frac{1}{n}=2\pi\left(\sum_{i=1}^{s}\frac{a_i}{p_i}+\frac{b}{2^m}\right)$$

$$=\sum_{i=1}^{s}\frac{a_i2\pi}{p_i}+\frac{b2\pi}{2^m},$$

此处 a_i及 b 都是整数。因为 p_i是费马素数，所以角 $2\pi/p_i$可以作出。又任意角皆可二等分，所以$2\pi/2^m$也可作出。显然，这些角的倍角 $a_i\times2\pi/p_i$及 $b\times2\pi/2^m$也可作出，其和、差也能作出。于是角$2\pi/n$ 也可作出了。

总结上面所述，我们得出：正 n 边形可以作出的充要条件是

$$n=p_1p_2\cdots p_s2^m,$$

其中 $p_1,p_2,\cdots,p_s$是互异的费马素数。

例15 我们可以应用例14的讨论，得出作正十七边形的步骤。请注意，$17=2^{2^2}+1$是一个费马素数。取$\zeta=e^{2\pi i/17}$，它是下面的十七次割圆多项式的根：

$$\varphi_{17}(x)=\frac{x^{17}-1}{x-1}=x^{16}+x^{15}+\cdots+x+1.$$

其余的15个根是$\zeta^2,\zeta^3,\cdots,\zeta^{16}$。令 $L=\mathbf{Q}[\zeta]$，则L是 $\mathbf{Q}$ 的伽罗瓦扩域.

$$o(G(L/\mathbf{Q}))=[L:\mathbf{Q}]=16.$$

令 $\sigma\in G(L/\mathbf{Q})$定义如下：

$$\sigma(\zeta)=\zeta^3.$$

于是 σ 对 $\varphi_{17}(x)$的16个根的作用如下：

$$\begin{aligned}\sigma:\ \zeta &\mapsto \zeta^3 \mapsto \zeta^9 \mapsto \zeta^{27}=\zeta^{10} \mapsto \zeta^{30}=\zeta^{13} \mapsto \zeta^{39}=\zeta^5 \mapsto \zeta^{15}\\ &\mapsto \zeta^{45}=\zeta^{11} \to \zeta^{33}=\zeta^{16} \mapsto \zeta^{48}=\zeta^{14}\\ &\mapsto \zeta^{42}=\zeta^{8} \mapsto \zeta^{24}=\zeta^{7} \mapsto \zeta^{21}=\zeta^{4} \mapsto \zeta^{12}\\ &\mapsto \zeta^{36}=\zeta^{2} \mapsto \zeta^{6} \mapsto \zeta^{18}=\zeta.\end{aligned}$$

所以 σ 的阶是16，故知 $G(L/\mathbf{Q})$ 是由 σ 生成的循环群．我们很容易得出 $G(L/\mathbf{Q})$ 的一个正规群列：

$$G(L/\mathbf{Q}) = \langle\sigma\rangle \rhd \langle\sigma^2\rangle \rhd \langle\sigma^4\rangle \rhd \langle\sigma^8\rangle \rhd \{e\}.$$

令

$$\begin{aligned}\alpha_8 &= \zeta + \zeta^{16},\\ \alpha_4 &= \zeta + \zeta^{13} + \zeta^{16} + \zeta^4,\\ \alpha_2 &= \zeta + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2,\\ \alpha_1 &= \sum_{i=1}^{16} \zeta^i = -1,\end{aligned}$$

则显然有

$$\sigma^8(\alpha_8) = \alpha_8, \quad \sigma^4(\alpha_4) = \alpha_4, \quad \sigma^2(\alpha_2) = \alpha_2, \quad \sigma(\alpha_1) = \alpha_1.$$

于是我们得出一系列的二次扩域：

$$\mathbf{Q} \subset \mathbf{Q}[\alpha_2] \subset \mathbf{Q}[\alpha_2, \alpha_4] \subset \mathbf{Q}[\alpha_2, \alpha_4, \alpha_8] \subset \mathbf{Q}[\zeta].$$

我们只要写出这些二次扩域的二次方程式就好了．例如，第一步，我们有

$$\begin{aligned}(x-\alpha_2)(x-\sigma(\alpha_2)) &= x^2 - \left(\sum_{i=1}^{16} \zeta^i\right)x + 4\sum_{i=1}^{16}\zeta^i\\ &= x^2 + x - 4 \in \mathbf{Q}[x],\end{aligned}$$

α_2 是上式的一个根．

读者不妨试行写出其余的三个二次式． ▎

下面的定理给出正规扩域的一个判别条件．

定理5.24 设 L 是 K 的一个有限代数扩域，Ω 是 L 的一个代数闭包．则 L 是 K 的正规扩域 $\Longleftrightarrow$ 任何一个 K 同构

$$\sigma:\ L \to \sigma(L) \subset \Omega$$

必然是L的K自同构。

证明 $\Longleftarrow$。设$L=K[a_1,\cdots,a_n]$，a_i $(i=1,\cdots,n)$对K的极小多项式是$f_i(x)$。令

$$f(x)=\prod_{i=1}^{n}f_i(x).$$

我们要证明$f(x)$在$L[x]$中可以分解成一次式的乘积。如此，则L是$f(x)$的分裂域，因而也是K的正规扩域。

如果有一个$f_i(x)$在$L[x]$中不能分解成一次式的乘积，不妨即设$f_1(x)$不能完全分解。于是，$f_1(x)$在Ω中有一根$\bar{a}_1$不在L中。按照定理5.9，存在一个K同构$\sigma_1: K[a_1]\to K[\bar{a}_1]\subset\Omega$，使

$$\sigma(a_1)=\bar{a}_1.$$

令a_2对$K[a_1]$的极小多项式为$g_2(x)$，$\bar{a}_2$为$\sigma_1(g_2(x))$在Ω中的一个根。又用定理5.9，于是存在一个K同构

$$\sigma_2: K[a_1,a_2]\to K[\bar{a}_1,\bar{a}_2]\subset\Omega,$$

使

$$\sigma_2(a_1)=\bar{a}_1,\qquad \sigma_2(a_2)=\bar{a}_2.$$

如此逐步作下去，即知在Ω中存在$\bar{a}_3,\cdots,\bar{a}_n$，以及一个$K$同构$\sigma_n$: $K[a_1,a_2,\cdots,a_n]\to K[\bar{a}_1,\bar{a}_2,\cdots,\bar{a}_n]$，使

$$\sigma_n(a_i)=\bar{a}_i,\qquad \forall i=1,2,\cdots,n.$$

因为$\bar{a}_1\bar{\in}L$，所以σ_n不是L的自同构，这与已知的条件相矛盾。

$\Longrightarrow$。设$L=K[a_1,\cdots,a_n]$，a_i对K的极小多项式是$f_i(x)$。按照已知条件，$f_i(x)$在$L[x]$中可分解成一次式的乘积。任取一个K同构σ: $L\to\sigma(L)\subset\Omega$。则有

$$0=\sigma(f_i(a_i))=f_i(\sigma(a_i)).$$

于是导出$\sigma(a_i)\subset L$。所以σ是L的一个K自同构。▍

上面这个定理，说明了正规扩域对K同构而言自成一个天地。下面我们要研究另一个有关伽罗瓦扩域的现象。设L是K的伽罗瓦扩域，Ω是L的代数闭包。在Ω中，另有K的一个扩域

S. 我们可以取包含L及S的最小的域

$$L\cdot S=S[L]=\left\{\sum_{\text{有限}}a_i\alpha_i:\ a_i\in S,\ \alpha_i\in L\right\},$$

$L\cdot S$ 称为 L,S 的**合成域**。

定理5.25 设L是K的伽罗瓦扩域，则合成域$L\cdot S$是S的一个伽罗瓦扩域，且$G(L\cdot S/S)$是$G(L/K)$的一个子群。

证明 因为L是K的伽罗瓦扩域，所以$L=K[\alpha]$。设α对K的极小多项式是$f(x)$，则$L\cdot S=S[\alpha]$是$f(x)$对S的分裂域。显然，$L\cdot S$是S的伽罗瓦扩域。

令$\sigma\in G(L\cdot S/S)$。则σ在L上的作用引生一个K同构

$$\bar\sigma:\ L\to\sigma(L)\subset\Omega.$$

按照上定理，$\bar\sigma$是L的一个K自同构。因此$\bar\sigma\in G(L/K)$。

我们要证明这个对应关系$\sigma\mapsto\bar\sigma$是一个单射。如果$\bar\sigma$为恒等映射，则必有

$$\sigma(\alpha)=\bar\sigma(\alpha)=\alpha.$$

于是σ也必是恒等映射。在此单射下，我们可以把$G(L\cdot S/S)$认同成$G(L/K)$的子群。▎

例16 设域K的特征是0，L是下面的方程式对K的分裂域：

$$x^n-1=0.$$

则L显然是K的伽罗瓦扩域。我们要证明$G(L/K)$是乘法群

$$\boldsymbol{Z}_n^*=\{[m]_n:\ (m,n)=(1)\}$$

的子群，所以是一个有限交换群。

x^n-1在L中的所有根的集合显然是一个n阶乘法群，所以是一个循环群(定理5.12)。令ζ为其生成元，则此群$=\{1,\zeta,\zeta^2,\cdots,\zeta^{n-1}\}$。故$L=K[\zeta]$。

我们考虑$Q\subset Q[\zeta]$。按照例7的讨论，ζ的极小多项式是n次割圆多项式$\varphi_n(x)$，其次数为尤拉数$\varphi(n)$，其根的集合为$\{\zeta^m:\ (m,n)=(1)\}$，所以

$$\varphi_n(x)=\prod_{\substack{0<m<n\\(m,n)=(1)}}(x-\zeta^m).$$

所以 $G(\mathbf{Q}[\zeta]/\mathbf{Q})=\{\sigma_m: 0<m<n, (m,n)=(1)\}$，其中 σ_m 的定义如下：

$$\sigma_m(\zeta)=\zeta^m.$$

显然，映射

$$\pi: G(\mathbf{Q}[\zeta]/\mathbf{Q})\to \mathbf{Z}_n^*,$$
$$\pi(\sigma_m)=[m]_n$$

是一个同构。

因为K的特征为0，故可认为 $K\supset\mathbf{Q}$. 而

$$L=K[\zeta]=\mathbf{Q}[\zeta]\cdot K,$$

所以应用定理5.25，立得 $G(L/K)$是 $\mathbf{Z}_n^*$的一个子群。

习　题

1. 设域K的特征 $p>0$，证明多项式 $x^p-x-a\in K[x]$是不可约的或是一次式的乘积。

2. 设 L 是K的有限扩域. 证明 L 是K 的正规扩域$\Longleftrightarrow$对于$K[x]$的一个不可约多项式 $f(x)$,如它在 $L[x]$内有两个因子$g(x)$, $h(x)$，则必有 $\deg g(x)=\deg h(x)$.

3. 证明一个 n 次多项式的分裂域可由它的任意 $n-1$ 个根生成(即添加任意 $n-1$个根到基域即得其分裂域)。

4. 设 $f(x)\in K[x]$，在K的扩域 L 内，$f(x)$分解为

$$f(x)=(x-u_1)^{n_1}\cdots(x-u_k)^{n_k}\quad(u_i\neq u_j, n_i\geqslant 1).$$

令 $v_0,\cdots,v_k$ 为多项式 $g(x)=(x-u_1)\cdots(x-u_k)$的系数，又设 $F=K(v_0,\cdots,v_k)$. 证明：

(1) L是 $g(x)$对 F的分裂域；

(2) L是F 的伽罗瓦扩域.

5. 设 L 是 $x^{10}-1$在 $\mathbf{Q}$ 上的分裂域. 求$[L:\mathbf{Q}]$，并问 $L/\mathbf{Q}$

的伽罗瓦群是否是循环群？

6．设L是$x^{15}-1$在$\mathbf{Q}$上的分裂域．求$[L:\mathbf{Q}]$，并问$L/\mathbf{Q}$的伽罗瓦群是否是循环群？

7．设K是一个有限域，$\overline{K}$是它的一个代数闭包．σ是$\overline{K}/K$的一个非幺自同构，那么，σ的不变域是有限域吗？

8．设$\overline{\mathbf{Q}}$为$\mathbf{Q}$的代数闭包，$u\in\overline{\mathbf{Q}}\backslash\mathbf{Q}$，证明在所有适合条件$\overline{\mathbf{Q}}\supset F$，$u\overline{\in}F$的域$F$中，必有一极大者．

9．续上题．设F是上题中所述极大中间域，证明F的任何有限扩域必为伽罗瓦扩域，而且其伽罗瓦群是循环群．

10．设F是x^4-2对$\mathbf{Q}$的分裂域．试找出F的所有子域，并列出它们的包含关系．

11．找出x^3-9对：

(1) $\mathbf{Q}$；(2) $\mathbf{Q}(\sqrt{2})$；(3) $\mathbf{Q}(\sqrt{-3})$的分裂域．

12．设F是题8，题9所述的极大中间子域，证明存在$\overline{\mathbf{Q}}$的自同构σ，使$\sigma(u)\neq u$，而且F为其不变域．

13．令a_{ij} $(i,j=1,2,\cdots,n)$为整数，使$\det(a_{ij})\neq0$．又设$x_1,\cdots,x_n$为变元，$L=\mathbf{C}(x_1,\cdots,x_n)$，$y_j=\prod\limits_{i=1}^{n}x_i^{a_{ij}}$．又令$K=\mathbf{C}(y_1,\cdots,y_n)$．证明$L$是$K$的代数扩域，并求$[L:K]$．再进一步证明$L$是$K$的伽罗瓦扩域．问其伽罗瓦群应如何计算？

14．设L是K的扩域，$K[\alpha]$是K的伽罗瓦扩域，证明$K[\alpha]$对K的伽罗瓦群等于$L[\alpha]$对L的伽罗瓦群的充要条件是

$$K[\alpha]\cap L=K.$$

15．求$\mathbf{Q}(e^{2\pi i/7})$对$\mathbf{Q}$的伽罗瓦群的所有子群和每个子群的不动域．

16．设α是$x^3+x^2-2x-1=0$的一个根，证明$\mathbf{Q}(\alpha)$是$\mathbf{Q}$的正规扩域，并求其伽罗瓦群．

17．设K是一个特征p的域，$p>0$．又设$\alpha\in K$，且不存在$\beta\in K$使$\alpha=\beta^p-\beta$．令L是$x^p-x-\alpha$的分裂域，求L/K的伽罗

瓦群。

18. 求 x^4-5在：

(1) Q； (2) $Q(\sqrt{5})$； (3) $Q(\sqrt{-5})$上的伽罗瓦群。

§7 用根式解方程式

任给一个二次式

$$ax^2+bx+c=0,$$

我们知道其根为

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}.$$

上式的解用到了根式$\sqrt{b^2-4ac}$。在巴比伦、埃及、中国、印度、希腊等古数学里，都有上面这个二次式的解法。祖冲之（五世纪）提出了“开带从立方”。可惜原书《缀术》已经失传了。按照字义来说，这应该是指“开带一个系数的立方根”，即解三次方程式

$$x^3+ax=b \quad 或 \quad x^3+ax^2=b.$$

十六世纪时，Cardan 公式给出三次及四次式的解：首先简化任意三次式为

$$x^3+ax+b=0,$$

则其一根（另外两根也很类似，见后文）为

$$\alpha=\sqrt[3]{-\frac{b}{2}+\sqrt{\frac{b^2}{4}+\frac{a^3}{27}}}+\sqrt[3]{-\frac{b}{2}-\sqrt{\frac{b^2}{4}+\frac{a^3}{27}}}.$$

这也是用根式求出解答。四次式的解也可以类似地用根式求出。

一般的五次式或更高次式，能不能用根式求解呢？答案是否定的，本节将给出证明。从分析学上看，我们知道任意的五次实系数方程式最少有一个实数根，并且可以用逐次逼近取极限的办法求解。在这种意义下，任意的五次式皆可解。就像三等分角的

问题一样，如不限定圆规直尺作图法，则任意角是可以三等分的。然而在圆规直尺作图的限制下，我们已知道至少有一个角不能三等分。用根式解方程式也类似，自然是限定用根式的方法。

我们要把用根式解方程式与伽罗瓦理论联系起来。为了简便起见，我们假定域K的特征是零。我们先引入下面的一些定义。

定义5.15 如果域L是下面的方程式对K的分裂域，则称L是K的**根式扩域**：

$$x^n - a = 0, \quad a \in K.$$

定义5.16 如果存在一个根式扩域的链

$$K = K_1 \subset K_2 \subset \cdots \subset K_i \subset K_{i+1} \subset \cdots \subset K_n,$$

即K_{i+1}是K_i的根式扩域($\forall i = 1, 2, \cdots, n-1$)，使$K[x]$中的一个多项式$f(x)$的分裂域$L \subset K_n$，则称$f(x)$**可以用根式求解**。

在证明本节的主要定理之前，我们先处理两个简单的情形。

定理5.26 如果域L是域K的根式扩域，则$G(L/K)$是可解群。

证明 取L的一个代数闭包Ω。则下式对K的分裂域$K[\zeta] \subset \Omega$是K的伽罗瓦扩域(见例16)：

$$x^n - 1 = 0.$$

而且$G(K[\zeta]/K)$是交换群。

设L是下式的分裂域：

$$x^n - a = 0, \quad a \in K,$$

α是其一根。则显然有

$$L = K[\alpha, \alpha\zeta, \alpha\zeta^2, \cdots, \alpha\zeta^{n-1}] = K[\alpha, \zeta].$$

我们要证明$G(L/K[\zeta])$也是一个交换群。

任取$\sigma \in G(L/K[\zeta])$，则显然σ是由下式确定的：

$$\sigma(\alpha) = \alpha\zeta^j, \quad 0 \leqslant j \leqslant n-1.$$

令如此决定的j为$j(\sigma)$。我们定义映射

$$\pi: G(L/K[\zeta]) \to \boldsymbol{Z}_n,$$

$$\pi(\sigma) = [j(\sigma)],$$

其中 $\boldsymbol{Z}_n$ 为加法群。不难看出 π 是一个群单射。所以 $G(L/K[\zeta])$ 可以认同为 $\boldsymbol{Z}_n$ 的一个子群，因此是交换群。

按照伽罗瓦理论的基本定理，我们有

$$G(L/K) \rhd G(L/K[\zeta]) \rhd \{e\},$$
$$G(L/K)/G(L/K[\zeta]) \approx G(K[\zeta]/K).$$

根据定义2.21，即知 $G(L/K)$ 是可解群。▌

定理5.27 如果 L 是多项式 $f(x)$ 对域 K 的分裂域，并且 $G(L/K)$ 是循环群，则 $f(x)$ 可以用根式求解。

证明 设 $n = o(G(L/K))$。Ω 是 L 的一个代数闭包。令 ζ 为下面的方程式在 Ω 中的一个根：

$$x^n - 1 = 0.$$

参见例16，我们可以取 ζ，使

$$x^n - 1 = \prod_{i=0}^{n-1}(x - \zeta^i).$$

于是 $K[\zeta]$ 是 $x^n - 1$ 对 K 的分裂域，故是 K 的根式扩域。

在 L 中取 α，使 $L = K[\alpha]$。又令 $L' = K[\alpha, \zeta]$。根据定理5.25，L' 是 $K[\zeta]$ 的伽罗瓦扩域，$G(L'/K[\zeta])$ 是 $G(L/K)$ 的子群。由于 $G(L/K)$ 是循环群，所以 $G(L'/K[\zeta])$ 也是循环群。令其生成元为 δ，其阶为 m，则 $m|n$，且有

$$G(L'/K[\zeta]) = \{1, \delta, \cdots, \delta^{m-1}\}.$$

令 $\eta = \zeta^{n/m}$，则有 $\eta^m = 1$。再令

$$(1)\quad \beta = \eta^m\alpha + \eta^{m-1}\delta(\alpha) + \cdots + \eta^{m-i}\delta^i(\alpha) + \cdots + \eta\delta^{m-1}(\alpha),$$

则有

$$\begin{aligned}(2)\quad \delta(\beta) &= \eta^m\delta(\alpha) + \eta^{m-1}\delta^2(\alpha) + \cdots + \eta^{m-i}\delta^{i+1}(\alpha) + \cdots + \eta\delta^m(\alpha) \\ &= \eta\alpha + \eta^m\delta(\alpha) + \cdots + \eta^{m-i+1}\delta^i(\alpha) + \cdots + \eta^2\delta^{m-1}(\alpha) \\ &= \eta\beta.\end{aligned}$$

故
$$\delta(\beta^m) = \delta(\beta)^m = (\eta\beta)^m = \eta^m\beta^m = \beta^m.$$

所以 $\beta^m \subset K[\zeta]$. 易见

$$x^m - \beta^m = \prod_{j=0}^{m-1}(x - \eta^j \beta),$$

故 $K[\beta,\zeta]$是 $x^m - \beta^m$对 $K[\zeta]$的分裂域，也即是 $K[\zeta]$的根式扩域。

我们要证明 $L' = K[\alpha,\zeta] = K[\beta,\zeta]$. 显然 $\beta \in L'$，所以

$$K[\alpha,\zeta] \supseteq K[\beta,\zeta].$$

另一方面，由（2）式知

$$\delta^j(\beta) = \delta^{j-1}\delta(\beta) = \delta^{j-1}(\eta\beta) = \eta\delta^{j-1}(\beta) = \cdots = \eta^j\beta,$$

故$1,\delta,\delta^2,\cdots,\delta^{m-1}$在 $K[\beta,\zeta]$上的作用都互不相同，所以

$$m \leqslant o(G(K[\beta,\zeta]/K[\zeta])) = [K[\beta,\zeta]:K[\zeta]]$$
$$\leqslant [K[\alpha,\zeta]:K[\zeta]] = m,$$

即有 $K[\beta,\zeta] = K[\alpha,\zeta]$.

于是我们得到了一个根式扩域的链：

$$K \subset K[\zeta] \subset K[\beta,\zeta],$$

且有
$$L \subset K[\alpha,\zeta] = K[\beta,\zeta].$$

所以 $f(x)$可用根式求解。▍

上面的定理5.26及定理5.27是证明定理5.30所给出的用根式求解的充要条件的开始。在扩充这两个定理以完成定理5.30的证明之前，我们需要下面两个技术性的引理。

引理1 设下面是一个根式扩域的链

$$K = K_1 \subset K_2 \subset \cdots \subset K_n,$$

则存在另一个根式扩域的链

$$K = L_1 \subset L_2 \subset \cdots \subset L_m,$$

使 $K_n \subset L_m$，且 L_m是K的伽罗瓦扩域。

证明 我们对第一个链的长度 n 作数学归纳法。设 $n=2$。因为 K_2是 K_1的伽罗瓦扩域，所以取 $L_2 = K_2$就可以了。现在我们假设对 K_{n-1}已作好了一个根式扩域的链

$$K = L_1 \subset L_2 \subset \cdots \subset L_{m'},$$

使 $K_{n-1} \subset L_{m'}$ 以及 $L_{m'}$ 是 K 的伽罗瓦扩域。

设 K_n 是下面的方程式对 K_{n-1} 的分裂域:

$$x^l - a = 0, \quad a \in K_{n-1} \subset L_{m'}.$$

令

$$f(x) = \prod_{\sigma \in G(L_{m'}/K)} (x^l - \sigma(a)).$$

则显然有 $\sigma(a) \in L_{m'}$, $f(x) \in K[x]$。对 $f(x)$ 的因元 $x^l - \sigma(a)$ 一个一个地从 $L_{m'}$ 开始作根式扩域，则得出下列根式扩域的链:

$$K = L_1 \subset L_2 \subset \cdots \subset L_{m'} \subset \cdots \subset L_m.$$

我们显然有 $K_n \subset L_m$。又因为 $L_{m'}$ 是 K 的伽罗瓦扩域，故可以设

$$L_{m'} = K[\alpha],$$

设 α 对 K 的极小多项式是 $g(x)$，则 L_m 显然是 $f(x)g(x) \subset K[x]$ 的分裂域，所以 L_m 是 K 的伽罗瓦扩域。∎

现在我们可以证明定理5.30中所述条件的必要性了。

定理5.28 任取非常数的多项式 $f(x) \in K[x]$。如果 $f(x)$ 可用根式求解，则 $G(L/K)$ 是可解群，此处 L 是 $f(x)$ 对 K 的分裂域。

证明 根据定义5.16，存在一个根式扩域的链:

$$K = K_1 \subset K_2 \subset \cdots \subset K_n,$$

使 $L \subset K_n$。应用上面的引理1，存在另一个根式扩域的链:

$$K = L_1 \subset L_2 \subset \cdots \subset L_m,$$

使 $K_n \subset L_m$，L_m 是 K 的伽罗瓦扩域。于是 $L \subset L_m$。L 自然是 K 的伽罗瓦扩域。按照伽罗瓦理论的基本定理，我们知道

$$G(L_m/K) \rhd G(L_m/L) \rhd \{e\},$$

$$G(L/K) \simeq G(L_m/K)/G(L_m/L).$$

应用定理2.22，我们仅须证明 $G(L_m/K)$ 是一个可解群。

再次应用伽罗瓦理论，我们得出一个群列如下:

$$G(L_m/K) \supset G(L_m/L_2) \supset \cdots \supset G(L_m/L_m) = \{e\}.$$

因为 L_{i+1} 是 L_i 的根式扩域，所以是伽罗瓦扩域。于是我们恒有

$$G(L_m/L_i) \triangleright G(L_m/L_{i+1}).$$

所以上面的群列是正规群列。其商群形如

$$G(L_m/L_i)/G(L_m/L_{i+1}) \approx G(L_{i+1}/L_i).$$

由定理5.26，知 $G(L_{i+1}/L_i)$ 为可解群。于是不难把这个正规群列加细为商群集是交换群集的一个正规群列。所以 $G(L_m/K)$ 是可解群。 ▎

引理2 设 S 是 K 的扩域，L 是 S 的扩域，以及存在 K 的一个根式扩域的链和 S 的一个根式扩域的链如下：

$$K = S_1 \subset S_2 \subset \cdots \subset S_n, \qquad S = L_1 \subset L_2 \subset \cdots \subset L_m,$$

使得 $S \subset S_n$，$L \subset L_m$。则存在 K 的一个根式扩域的链

$$K = K_1 \subset K_2 \subset \cdots \subset K_l,$$

使 $L \subset K_l$。

证明 设 L_i 是下面的多项式对 L_{i-1} 的分裂域：

$$f_i(x) = x^{m_i} - a_i, \qquad a_i \in L_{i-1}.$$

令 $K_j = S_j (j = 1, 2, \cdots, n)$，$K_{n+1}$ 为 $f_2(x)$ 对 K_n 的分裂域，…，K_{n+i} 为 $f_{i+1}(x)$ 对 K_{n+i-1} 的分裂域，…，K_{n+m-1} 是 $f_m(x)$ 对 K_{n+m-2} 的分裂域。则显然有 $K_{n+1} \supset L_2, \cdots, K_{n+i} \supset L_{i+1}, \cdots, K_{n+m-1} \supset L_m \supset L$。于是

$$K = K_1 \subset K_2 \subset \cdots \subset K_{n+m-1}$$

即是我们所要求的链。 ▎

现在我们证明定理5.30中所述条件的充分性。

定理5.29 任取非常数的多项式 $f(x) \in K[x]$。设 L 是 $f(x)$ 对 K 的分裂域。如果 $G(L/K)$ 是可解群，则 $f(x)$ 可以用根式求解。

证明 如果 $G(L/K)$ 是可解群，则存在一个正规群列，使其商群都是交换群。把这个正规群列细化以后，可以使其商群都是循环群。设此细化后的正规群列为

$$G(L/K) \triangleright H_{n-1} \triangleright H_{n-2} \triangleright \cdots \triangleright H_0 = \{e\}.$$

应用伽罗瓦理论的基本定理，则知与此群列相对应的，有一个中

间域的链

$$K \subset K_1 \subset K_2 \subset \cdots \subset K_n = L,$$

其中K_{i+1}是K_i的伽罗瓦扩域，且$G(K_{i+1}/K_i)$是循环群。设K_{i+1}是多项式$f_{i+1}(x) \in K_i[x]$对K_i的分裂域，根据定理5.27及定义5.16，存在K_i的一个根式扩域的链，使K_{i+1}含于此链中的最大的域。反复应用引理2，不难看出，存在K的一个根式扩域的链

$$K = L_1 \subset L_2 \subset \cdots \subset L_t,$$

使$L \subset L_t$。于是，按照定义5.16，$f(x)$可以用根式求解。▎

综合上面两个定理，立得下面的定理：

定理5.30（伽罗瓦定理） 任取非常数的多项式$f(x) \in K[x]$。设$f(x)$对K的分裂域为L。则$f(x)$可以用根号求解的充要条件是：$G(L/K)$是可解群。

证明 应用定理5.28及定理5.29。▎

例17 我们应用上面的推理过程，用根式解三次式，以导出本节开始所提到的Cardan公式。

假设域K有三次单位根$\zeta \neq 1$。设$\alpha_1, \alpha_2, \alpha_3$都是变数，其初等对称多项式为

$$\theta_1 = \alpha_1 + \alpha_2 + \alpha_3, \quad \theta_2 = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3, \quad \theta_3 = \alpha_1\alpha_2\alpha_3.$$

在$K(\theta_1, \theta_2, \theta_3)[x]$中取下面的多项式

$$f(x) = \prod_{i=1}^{3}(x - \alpha_i) = x^3 - \theta_1 x^2 + \theta_2 x - \theta_3.$$

我们的目的无非是将$\alpha_1, \alpha_2, \alpha_3$用$\zeta$及$\theta_1, \theta_2, \theta_3$的根式表出。

易见$f(x)$对$K(\theta_1, \theta_2, \theta_3)$的分裂域是$K(\alpha_1, \alpha_2, \alpha_3)$。且

$$G(K(\alpha_1, \alpha_2, \alpha_3)/K(\theta_1, \theta_2, \theta_3)) = S_3$$

（请读者参看第三章§4定理3.16后的讨论）。在S_3中存在一正规群列：

$$S_3 \rhd A_3 \rhd \{e\}.$$

不难看出S_3是一个可解群。与上面的正规群列相对应的是下面的

域的链：

$$K(\theta_1,\theta_2,\theta_3)\subset L\subset K(\alpha_1,\alpha_2,\alpha_3).$$

容易确定L。事实上，$[L:K(\theta_1,\theta_2,\theta_3)]=o(S_3/A_3)=2$。令

$$D=(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1),$$

显然D不是一个对称多项式，所以不在$K(\theta_1,\theta_2,\theta_3)$之中，但$D$在$A_3$作用下是不变的，故$D\in L$。由此即知

$$L=K(\theta_1,\theta_2,\theta_3)(D).$$

D对$K(\theta_1,\theta_2,\theta_3)$的极小多项式是(参见第三章例7)

$$g(x)=x^2-D^2=x^2+4\theta_1^3\theta_3-\theta_1^2\theta_2^2-18\theta_1\theta_2\theta_3+4\theta_2^3+27\theta_3^2.$$

于是可令

$$D=\sqrt{-4\theta_1^3\theta_3+\theta_1^2\theta_2^2+18\theta_1\theta_2\theta_3-4\theta_2^3-27\theta_3^2}.$$

令$\sigma=(1,2,3)$以及

(1) $$\beta=\alpha_1+\sigma(\alpha_1)\zeta^2+\sigma^2(\alpha_1)\zeta=\alpha_1+\alpha_2\zeta^2+\alpha_3\zeta,$$

则有

(2) $$\sigma(\beta)=\alpha_2+\alpha_3\zeta^2+\alpha_1\zeta=\beta\zeta,$$

(3) $$\sigma^2(\beta)=\alpha_3+\alpha_1\zeta^2+\alpha_2\zeta=\beta\zeta^2.$$

显然$\sigma(\beta^3)=(\sigma(\beta))^3=\beta^3\zeta^3=\beta^3$，所以$\beta^3\in L=K(\theta_1,\theta_2,\theta_3)(D)$。我们把$\beta^3$具体地写出来。由(1)式，经过计算，并注意到

$$\zeta^2+1/2=-(\zeta+1/2),$$

即有

$$\beta^3=\theta_1^3-\frac{9}{2}(\theta_1\theta_2-3\theta_3)+3\left(\zeta+\frac{1}{2}\right)D.$$

于是可令

$$\beta=\sqrt[3]{\theta_1^3-\frac{9}{2}(\theta_1\theta_2-3\theta_3)+3\left(\zeta+\frac{1}{2}\right)D}\,\zeta^j,\quad j=0,1,2.$$

又令

(4) $$\gamma=\alpha_1+\sigma(\alpha_1)\zeta+\sigma^2(\alpha_1)\zeta^2=\alpha_1+\alpha_2\zeta+\alpha_3\zeta^2,$$

则不难看出

$$\sigma(\gamma)=\alpha_2+\alpha_3\zeta+\alpha_1\zeta^2=\gamma\zeta^2,$$

以及

$$\sigma(\beta\gamma)=\beta\zeta\gamma\zeta^2=\beta\gamma.$$

于是$\gamma^3, \beta\gamma \subset K(\theta_1, \theta_2, \theta_3)(D)$。把$\gamma^3, \beta\gamma$具体地写出来，有

$$\gamma^3 = \theta_1^3 - \frac{9}{2}(\theta_1\theta_2 - 3\theta_3) - 3\left(\zeta + \frac{1}{2}\right)D,$$

$$\beta\gamma = \theta_1^2 - 3\theta_2.$$

给定β的一个值以后，上二式可以确定γ的值。

利用(1)，(4)二式以及下式

$$\theta_1 = \alpha_1 + \alpha_2 + \alpha_3,$$

解联立线性方程式，可以求出$\alpha_1, \alpha_2, \alpha_3$的值如下：

$$\alpha_1 = \frac{1}{3}(\theta_1 + \beta + \gamma),$$

$$\alpha_2 = \frac{1}{3}(\theta_1 + \beta\zeta^2 + \gamma\zeta), \tag{5}$$

$$\alpha_3 = \frac{1}{3}(\theta_1 + \beta\zeta + \gamma\zeta^2).$$

在上面所得出的结果中，如果以常数$\bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3$代替变数$\alpha_1, \alpha_2, \alpha_3$，则相应地有常数的$\bar{\theta}_1, \bar{\theta}_2, \bar{\theta}_3$。而(5)式显然给出

$$f(x) = x^3 - \bar{\theta}_1 x^2 + \bar{\theta}_2 x - \bar{\theta}_3$$

的三个根。

如果在$f(x) = x^3 - \theta_1 x^2 + \theta_2 x - \theta_3$中，以$x + \theta_1/3$代替$x$，则$x^2$项的系数变为0。因此，我们不妨假设$\theta_1 = 0$，以简化多项式。此时，我们有

$$D = \sqrt{-4\theta_2^3 - 27\theta_3^2},$$

$$\beta^3 = \frac{27}{2}\theta_3 + \frac{3}{2}\sqrt{-3}D \quad \left(注意\ \zeta + \frac{1}{2} = \frac{1}{2}\sqrt{-3}\right),$$

$$\gamma^3 = \frac{27}{2}\theta_3 - \frac{3}{2}\sqrt{-3}D,$$

$$\alpha_1 = \frac{1}{3}(\beta + \gamma) = \sqrt[3]{\frac{\theta_3}{2} + \sqrt{\frac{\theta_3^2}{4} + \frac{\theta_2^3}{27}}} + \sqrt[3]{\frac{\theta_3}{2} - \sqrt{\frac{\theta_3^2}{4} + \frac{\theta_2^3}{27}}},$$

$$\alpha_2 = \sqrt[3]{\frac{\theta_3}{2} + \sqrt{\frac{\theta_3^2}{4} + \frac{\theta_2^3}{27}}}\zeta^2 + \sqrt[3]{\frac{\theta_3}{2} - \sqrt{\frac{\theta_3^2}{4} + \frac{\theta_2^3}{27}}}\zeta,$$

$$\alpha_3 = \sqrt[3]{\frac{\theta_3}{2} + \sqrt{\frac{\theta_3^2}{4} + \frac{\theta_2^3}{27}}}\zeta + \sqrt[3]{\frac{\theta_3}{2} - \sqrt{\frac{\theta_3^2}{4} + \frac{\theta_2^3}{27}}}\zeta^2.$$

即所谓Cardan公式。

例18 与例17类似，我们要用根式求解四次式。假设域F中有三次本原单位根ζ及四次本原单位根i。设$\alpha_1,\alpha_2,\alpha_3,\alpha_4$都是变数，其初等对称多项式为

$$(1)\quad \begin{aligned} \theta_1 &= \alpha_1+\alpha_2+\alpha_3+\alpha_4,\\ \theta_2 &= \alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_1\alpha_4+\alpha_2\alpha_3+\alpha_2\alpha_4+\alpha_3\alpha_4,\\ \theta_3 &= \alpha_1\alpha_2\alpha_3+\alpha_1\alpha_2\alpha_4+\alpha_1\alpha_3\alpha_4+\alpha_2\alpha_3\alpha_4,\\ \theta_4 &= \alpha_1\alpha_2\alpha_3\alpha_4. \end{aligned}$$

在$F(\theta_1,\theta_2,\theta_3,\theta_4)[x]$中取下面多项式

$$(2)\qquad f(x) = \prod_{j=1}^{4}(x-\alpha_j) = x^4-\theta_1x^3+\theta_2x^2-\theta_3x+\theta_4,$$

则$f(x)$对$F(\theta_1,\theta_2,\theta_3,\theta_4)$的分裂域是$F(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$。按照定理3.16后面的讨论，读者不难看出

$$G(F(\alpha_1,\alpha_2,\alpha_3,\alpha_4)/F(\theta_1,\theta_2,\theta_3,\theta_4)) = S_4.$$

在S_4中存在下面的正规群列

$$S_4 \rhd A_4 \rhd K \rhd N \rhd \{e\},$$

其中$K=\{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$，$N=\{e,(1,2)(3,4)\}$。由此立得$S_4$是一个可解群。与上面的正规群列相对应的，是下面的域的链：

$$F(\theta_1,\theta_2,\theta_3,\theta_4)\subset L_1\subset L_2\subset L_3\subset F(\alpha_1,\alpha_2,\alpha_3,\alpha_4).$$

显然，$[L_2:F(\theta_1,\theta_2,\theta_3,\theta_4)]=[S_4:K]=6$，故

$$G(L_2/F(\theta_1,\theta_2,\theta_3,\theta_4))$$

是循环群。所以我们可以跳过L_1，直接求出L_2。令

$$(3)\quad \beta_1=\alpha_1\alpha_2+\alpha_3\alpha_4,\qquad \beta_2=\alpha_1\alpha_3+\alpha_2\alpha_4,\qquad \beta_3=\alpha_1\alpha_4+\alpha_2\alpha_3,$$

则在K作用下，β_1,β_2,β_3皆不变，所以$\beta_1,\beta_2,\beta_3\in L_2$。而$S_4$作用在集合$\{\beta_1,\beta_2,\beta_3\}$上，成为$\{\beta_1,\beta_2,\beta_3\}$的变换群$S_3$，所以

$$
\begin{aligned}
(4)\qquad g(x)&=\prod_{j=1}^{3}(x-\beta_j)\\
&=x^3-(\beta_1+\beta_2+\beta_3)x^2+(\beta_1\beta_2+\beta_1\beta_3+\beta_2\beta_3)x\\
&\quad-\beta_1\beta_2\beta_3
\end{aligned}
$$

是$F(\theta_1,\theta_2,\theta_3,\theta_4)[x]$中的元素，于是$F(\theta_1,\theta_2,\theta_3,\theta_4)[\beta_1,\beta_2,\beta_3]$是$g(x)$对$F(\theta_1,\theta_2,\theta_3,\theta_4)$的分裂域，以及

$$[F(\theta_1,\theta_2,\theta_3,\theta_4)[\beta_1,\beta_2,\beta_3]:F(\theta_1,\theta_2,\theta_3,\theta_4)]\geqslant 6.$$

如此，我们得$L_2=F(\theta_1,\theta_2,\theta_3,\theta_4)[\beta_1,\beta_2,\beta_3]$。经计算后，得出

$$(5)\qquad g(x)=x^3-\theta_2x^2+(\theta_1\theta_3-4\theta_4)x-\theta_4(\theta_1^2-4\theta_2)-\theta_3^2.$$

用例17的方法，我们可以解(5)式，求出β_1,β_2,β_3。

我们要用β_1,β_2,β_3的值去求解$\alpha_1,\alpha_2,\alpha_3,\alpha_4$。引入

$$
(6)\qquad
\begin{aligned}
\gamma_1&=2(\alpha_1+\alpha_2)-\theta_1=\alpha_1+\alpha_2-\alpha_3-\alpha_4,\\
\gamma_2&=2(\alpha_1+\alpha_3)-\theta_1=\alpha_1-\alpha_2+\alpha_3-\alpha_4,\\
\gamma_3&=2(\alpha_1+\alpha_4)-\theta_1=\alpha_1-\alpha_2-\alpha_3+\alpha_4.
\end{aligned}
$$

任取$\sigma\in K$，不难看出$\sigma(\gamma_j)=\pm\gamma_j(j=1,2,3)$。所以$\gamma_j^2\in L_2$。经计算，有

$$
(7)\qquad
\begin{aligned}
\gamma_1^2&=\theta_1^2-4\theta_2+4\beta_1,\\
\gamma_2^2&=\theta_1^2-4\theta_2+4\beta_2,\\
\gamma_3^2&=\theta_1^2-4\theta_2+4\beta_3,
\end{aligned}
$$

以及

$$(8)\qquad \gamma_1\gamma_2\gamma_3=8\theta_3-4\theta_1\theta_2+\theta_1^3.$$

任取$\gamma_1,\gamma_2,\gamma_3$适合(7)与(8)式，则$\alpha_1,\alpha_2,\alpha_3,\alpha_4$可以写出如下：

$$
(9)\qquad
\begin{aligned}
\alpha_1&=\frac{1}{4}(\theta_1+\gamma_1+\gamma_2+\gamma_3),\quad \alpha_2=\frac{1}{4}(\theta_1+\gamma_1-\gamma_2-\gamma_3),\\
\alpha_3&=\frac{1}{4}(\theta_1-\gamma_1+\gamma_2-\gamma_3),\quad \alpha_4=\frac{1}{4}(\theta_1-\gamma_1-\gamma_2+\gamma_3).\ \blacksquare
\end{aligned}
$$

在例19中，我们将给出一个不能用根式求解的有理系数的五次方程的例子。按照定理5.30，仅须证明其分裂域的自同构群$G(L,Q)$不是可解群。为此，我们需要下面的引理。

引理3 设p是一个素数，G是S_p的一个子群。如果G是**传递的**（即任给$i,j\in\{1,2,\cdots,p\}$，则存在$\sigma\in G$，使$\sigma(i)=j$），以及有一对换$(k,l)\in G$，则$G=S_p$。

证明 我们在$\{1,2,\cdots,p\}$中定义一个关系"～"：

$$i\sim j\Longleftrightarrow(i,j)\in G.$$

显然，我们有$i\sim i$，以及$i\sim j\Longrightarrow j\sim i$。又如果有

$$i\sim j,\quad j\sim k,$$

则
$$(i,k)=(j,k)(i,j)(j,k)\in G,$$

故$i\sim k$。于是，"～"是一个等价关系。令

$$E(i)=\{j:\ j\sim i\},$$

即i所在的等价类。对$\sigma\in G$，考虑σ在$E(i)$上的作用。不难看出$\sigma(E(i))\subset E(\sigma(i))$。事实上，设$j\in E(i)$，即$(i,j)\in G$，则

$$(\sigma(i),\sigma(j))=\sigma\circ(i,j)\circ\sigma^{-1}\in G,$$

即$\sigma(j)\in E(\sigma(i))$。同样地，$\sigma^{-1}(E(\sigma(i)))\subset E(i)$，且显然$\sigma^{-1}\circ\sigma$与$\sigma\circ\sigma^{-1}$分别为$E(i)$及$E(\sigma(i))$上的恒等映射，所以$E(i)$与$E(\sigma(i))$基数相同。而$G$是传递的，所以所有等价子集$E(i)$ $(i=1,2,\cdots,p)$的基数都相同。但集合$\{1,2,\cdots,p\}$的基数为素数p，所以$E(i)$的基数只能是1或p。注意到对换$(k,l)\in G$，即$E(k)$的基数至少为2，立得等价子集的基数为p，即只有一个等价子集。于是

$$(i,j)\in G,\qquad\forall\, i,j=1,2,\cdots,p.$$

应用定理2.23，立得本定理。▌

例19 我们举一个不能用根式求解的五次方程的例子。令

$$f(x)=2x^5-10x+5.$$

设L为$f(x)$对Q的分裂域。我们要证明$G(L,Q)=S_5$。如此，根据定理2.27，S_5不是可解群，再根据定理5.30，即知$f(x)$不能用

根号求解。

应用爱森斯坦判别定理，取 $p=5$，则立得$f(x)$是$\mathbf{Q}[x]$中的不可约多项式。在 $\mathbf{C}[x]$中，令

$$f(x)=2\prod_{i=1}^{5}(x-\alpha_i),$$

则有 $\sigma_{ij}:\mathbf{Q}[\alpha_i]\approx\mathbf{Q}[x]/(f(x))\approx\mathbf{Q}[\alpha_j]$ $(\forall i,j=1,2,\cdots,5)$。把$f(x)$在 $\mathbf{Q}[\alpha_i][x]$内分解成素元的乘积之后，不难看出，σ_{ij}可以逐步地扩张成由L到$\mathbf{C}$的$\mathbf{Q}$同构。然而L是 $\mathbf{Q}$ 的伽罗瓦扩域，应用定理5.24，即知 σ_{ij} 是L的 $\mathbf{Q}$ 自同构。这样，我们证明了$G(L/\mathbf{Q})$作用在$\{1,2,3,4,5\}$上是传递的。

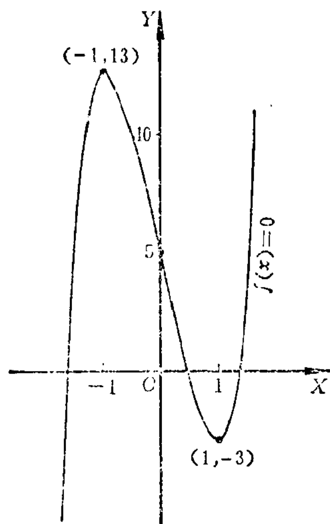


图 5.4

我们要证明$f(x)$有三个实根及两个非实根。应用初等微积分学的作图法，即可得到图5.4。请注意，

$$\lim_{x\to\infty}f(x)=\infty,$$

$$\lim_{x\to-\infty}f(x)=-\infty.$$

显然可见，$f(x)$有三个实根，设$\alpha+\beta\mathrm{i}$是 $f(x)$的另外一个根，此处$\alpha,\beta\in\mathbf{R}$，则在复共轭的作用下，

$$\overline{\alpha+\beta\mathrm{i}}=\alpha-\beta\mathrm{i},$$

$$0=\overline{f(\alpha+\beta\mathrm{i})}=f(\overline{\alpha+\beta\mathrm{i}})$$
$$=f(\alpha-\beta\mathrm{i}),$$

所以$\alpha-\beta\mathrm{i}$是$f(x)$的最后一个根。

复数域 $\mathbf{C}$ 的共轭，作用在域 L 上，自然是L的一个 $\mathbf{Q}$ 自同构，所以是$G(L/\mathbf{Q})$中的一个元素。它在$f(x)$的五个根上的作用是使其中两个根对换，即是S_5中的一个对换。又前面已经证明出

$G(L/\mathbf{Q})\subset S_5$ 是传递的，根据引理3，$G(L/\mathbf{Q})=S_5$。而 S_5 不是可解群，于是$f(x)$的根不能用根号解出。

习　　题

1. 设p是不等于域K的特征的素数，$a\in K$。证明x^p-a或者在$K[x]$内不可约，或者有一根属于K。

2. 设x^p-a(p为素数，$a\in\mathbf{Q}$)在$\mathbf{Q}[x]$内不可约，证明它对$\mathbf{Q}$的伽罗瓦群(即其分裂域在$\mathbf{Q}$上的伽罗瓦群)同构于$\mathbf{Z}/p\mathbf{Z}$上形如

$$y\mapsto ky+l\quad(k\neq 0)$$

的变换所组成的变换群。

3. 设F是特征为0的域，E是x^p-1(p为素数)在F上的分裂域，证明E可嵌入一个域K，使有一串F的扩域链：

$$F=F_1\subset F_2\subset\cdots\subset F_{r+1}=K,$$

其中$F_{i+1}=F_i(d_i)$，而$d_i^{n_i}=a_i\in F_i$，且K包含在F的一个分裂域中，其中n_i为素数。

4. 在上题中，设$F=\mathbf{Q}$，p分别是5及7，试求出所需要的域K及中间子域链。

5. 设K是域，$u_1,\cdots,u_n$是K上超越元。证明多项式

$$f(x)=x^n+u_1x^{n-1}+\cdots+u_n$$

在域$K(u_1,\cdots,u_n)$是可离的，且它对$K(u_1,\cdots,u_n)$的伽罗瓦群是S_n。

6. 试判断$x^5-3x+1=0$能否用根式求解。

§8　域多项式及判别式

设L是K的有限扩域，则L可看成一有限维的K向量空间：$L=\bigoplus Kw_i$。任给$a\in L$，用乘法定义L的一个线性变换A如下：

$$A(\alpha)=a\alpha,\qquad \alpha\in L.$$

令
$$aw_i = \sum_j a_{ij} w_j, \qquad a_{ij} \in K,$$

则元素 a 唯一地对应着一个线性变换A以及其矩阵$[a_{ij}]$. 这样，我们可以引用线性代数的定理来讨论代数扩域.

定义5.17 符号如上. 称A的特征多项式$\det(xI-A)$为 a **的域多项式**，这里$A=[a_{ij}]$.

讨论 1) a 的域多项式的次数等于$[L:K]$. 此域多项式显然是由a, L, K三者决定的. 如果有混淆的可能性，我们将标明 L 及 K.

2) 我们显然有

$$aI\begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix} = A\begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix},$$

即

$$(aI-A)\begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

于是，$\det(aI-A)=0$，也即 a 是它的域多项式的一个根.

3) a 的域多项式显然是与基元集$\{w_i\}$的选取无关的. ▌

我们要证明下面的定理.

定理5.31 令 a 的域多项式为 $F(x)$，极小多项式为 $f(x)$. 则有

1) 如果$L=K[a]$，则 $F(x)=f(x)$;

2) 令$m=[L:K[a]]$，则$F(x)=f(x)^m$.

证明 1) 应用上面的讨论 2)，立得

$$f(x) \mid F(x).$$

又因为$f(x)$与$F(x)$都是首一多项式，且$\deg f(x)=\deg F(x)$，所以必有$f(x)=F(x)$.

2) 令 $[K[a]:K]=s$，则$\{a^0=1,a,a^2,\cdots,a^{s-1}\}$是$K[a]$对$K$的一组基。令$\{v_1,v_2,\cdots,v_m\}$是$L$对$K[a]$的一组基，立得

$$\{1\times v_1,av_1,\cdots,a^{s-1}v_1,1\times v_2,\cdots,a^{s-1}v_2,\cdots,1\times v_m,\cdots,a^{s-1}v_m\}$$

是L对K的一组基。令

$$R_i=Kv_i\oplus Kav_i\oplus\cdots\oplus Ka^{s-1}v_i,\qquad i=1,2,\cdots,m.$$

则R_i是在a作用下的不变子空间，而且a对R_i的特征多项式是一样的($\forall i=1,2,\cdots,m$)。不妨令$v_1=1$。由 1)即知，a对R_1的特征多项式即是a对K的极小多项式$f(x)$。于是立得$F(x)=f(x)^m$。▎

就像在一般的线性代数理论中一样，令a对应的矩阵为

$$A=[a_{ij}]_{n\times n}.$$

我们定义“迹”和“范数”如下：

定义5.18 a的迹定义为$\mathrm{Tr}_{L/K}(a)=\sum_{i=1}^{n}a_{ii}$；$a$的范数定义为$\mathrm{N}_{L/K}(a)=\det A$。也即，如果$a$的域多项式为

$$F(x)=x^n+a_1x^{n-1}+\cdots+a_n,$$

则有

$$\mathrm{Tr}_{L/K}(a)=-a_1,\qquad \mathrm{N}_{L/K}(a)=(-1)^n a_n.$$

定理5.32 $\mathrm{Tr}_{L/K}$: $L\to K$是一个K线性映射，$\mathrm{N}_{L/K}$: $L\to K$是一个积性映射(即$\mathrm{N}_{L/K}(ab)=\mathrm{N}_{L/K}(a)\mathrm{N}_{L/K}(b)$)。我们还有，任取$k\in K$，则$\mathrm{Tr}_{L/K}(k)=nk$，$\mathrm{N}_{L/K}(k)=k^n$，此处$n=[L:K]$。

证明 显然。▎

例20 设$d\in\mathbf{Q}$，d不是一个有理数的平方。考虑$\mathbf{Q}(\sqrt{d})\supset\mathbf{Q}$。令$w_1=1$，$w_2=\sqrt{d}$。任取$a,b\in\mathbf{Q}$，则有

$$(a+b\sqrt{d})\times 1=a\times 1+b\sqrt{d},$$
$$(a+b\sqrt{d})\sqrt{d}=bd\times 1+a\sqrt{d}.$$

即
$$A=\begin{bmatrix} a & b\\ bd & a\end{bmatrix}.$$

其特征多项式为

$$\det\begin{bmatrix} x-a & -b \\ -bd & x-a \end{bmatrix} = (x-a)^2 - b^2d = x^2 - 2ax + (a^2 - b^2d).$$

于是

$$\mathrm{Tr}(a+b\sqrt{d}) = 2a = (a+b\sqrt{d}) + (a-b\sqrt{d}),$$

$$\mathrm{N}(a+b\sqrt{d}) = a^2 - b^2d = (a+b\sqrt{d})(a-b\sqrt{d}). \quad \blacksquare$$

我们有下面的关于一组基的判别式的定义。

定义5.19 设$\{w_1, w_2, \cdots, w_n\}$是$L$对$K$的一组基。则$\{w_1, w_2, \cdots, w_n\}$的判别式定义为

$$\mathrm{Dis}\{w_1, w_2, \cdots, w_n\} = \det[\mathrm{Tr}_{L/K}(w_i \cdot w_j)].$$

讨论 如果$\{w'_1, w'_2, \cdots, w'_n\}$是$L$对$K$的另一组基，令

$$w'_i = \sum_j b_{ij} w_j, \qquad \beta = [b_{ij}]_{n\times n},$$

则不难算出

$$\mathrm{Dis}\{w'_1, w'_2, \cdots, w'_n\} = \mathrm{Dis}\{w_1, w_2, \cdots, w_n\}(\det\beta)^2.$$

显然，基的判别式依赖于基的选取。可是，因为$\det\beta \neq 0$，所以，只要某一组基的判别式为零，则所有基的判别式就都为零。这就是说，基的判别式是否等于零，则是扩域$L\supset K$的性质了。 ▌

我们有下面的定理。

定理5.33 $\mathrm{Dis}\{w_1, w_2, \cdots, w_n\} \neq 0 \Longleftrightarrow L$是$K$的可离扩域。

证明 $\Longrightarrow$。参考定理5.20，令K_L^s为K在L中的可离代数闭包。如果$K_L^s \neq L$，则有

$$[L:K_L^s] = p^l, \qquad \alpha \in L\backslash K_L^s \Longrightarrow \alpha^{p^l} \in K_L^s.$$

其中p为域L的特征，$l \geqslant 1$。任取$\beta \in L$，令它对K的极小多项式为$f(x)$。如果$\beta \in L\backslash K_L^s$，设$\beta^{p^t} \in K_L^s$，但$\beta^{p^{t-1}} \notin K_L^s$，则$t \geqslant 1$，$x^{p^t} - \beta^{p^t}$在$K_L^s[x]$中不可约。再设$\beta^{p^t}$对$K$的极小多项式为$g(x)$，则有

$$f(x) = g(x^{p^t}).$$

令 $r=[L:K[\beta]]$，则 β 的域多项式为

$$F(x)=f(x)^r=g(x^{p^l})^r=x^n+0\times x^{n-1}+\cdots.$$

故
$$\mathrm{Tr}_{L/K}(\beta)=0.$$

若 $\beta\in K_L^s$，令 $r'=[K_L^s:K[\beta]]$，则

$$[L:K[\beta]]=[L:K_L^s][K_L^s:K[\beta]]=r'p^l.$$

于是

$$F(x)=f(x)^{r'p^l}=f(x^{p^l})^{r'}=x^n+0\times x^{n-1}+\cdots,$$

所以同样得出$\mathrm{Tr}_{L/K}(\beta)=0$。于是 $\mathrm{Tr}_{L/K}(w_iw_j)=0$，即有

$$\mathrm{Dis}(w_1,w_2,\cdots,w_n)=0.$$

$\Longleftarrow$. L是K的单扩域。令$L=K[\alpha]$，则$\{1,\alpha,\cdots,\alpha^{n-1}\}$是$L$的一组基。令 α 的极小多项式为 $f(x)$，则 α 的域多项式 $F(x)=f(x)$。任取 L的一个代数闭包 Ω。设 $f(x)$在 $\Omega[x]$中分解为

$$f(x)=\prod(x-\alpha_i),\qquad \alpha_1=\alpha,$$

其中 $\alpha_i\neq\alpha_j(i\neq j)$。易见

$$\mathrm{Tr}_{L/K}(\alpha)=\sum_i\alpha_i,\qquad \mathrm{Tr}_{L/K}(\alpha^l)=\sum_i\alpha_i^l.$$

于是

$$\mathrm{Dis}\{1,\alpha,\cdots,\alpha^{n-1}\}=\det\begin{bmatrix} n & \sum\alpha_i & \cdots & \sum\alpha_i^{n-1}\\ \sum\alpha_i & \sum\alpha_i^2 & \cdots & \sum\alpha_i^n\\ \cdots & \cdots & \cdots & \cdots\\ \sum\alpha_i^{n-1} & \sum\alpha_i^n & \cdots & \sum\alpha_i^{2n-2}\end{bmatrix}$$

$$=\det\begin{bmatrix}1 & 1 & \cdots & 1\\ \alpha_1 & \alpha_2 & \cdots & \alpha_n\\ \cdots & \cdots & \cdots & \cdots\\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1}\end{bmatrix}\det\begin{bmatrix}1 & \alpha_1 & \cdots & \alpha_1^{n-1}\\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1}\\ \cdots & \cdots & \cdots & \cdots\\ 1 & \alpha_n & \cdots & \alpha_n^{n-1}\end{bmatrix}$$

$$=\prod_{i>j}(\alpha_i-\alpha_j)^2\neq 0. \quad \blacksquare$$

习　　题

1. 设K是$\mathbf{Q}$的有限代数扩域，问

$$\mathrm{Tr}_{K/\mathbf{Q}}:\ K\to\mathbf{Q}$$

是否总是满射?

$$\mathrm{N}_{K/\mathbf{Q}}:\ K\to\mathbf{Q}$$

是否总是满射?

2. 设L是K的n次扩域，$L=K(\alpha)$。设α在K上的极小多项式$f(x)$的根为$\alpha_1=\alpha,\alpha_2,\cdots,\alpha_n$。对$L$中任一元素$\beta$，我们有：

$$\beta=a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}\quad(a_i\in K).$$

令

$$\beta_i=a_0+a_1\alpha_i+\cdots+a_{n-1}\alpha_i^{n-1}.$$

证明

$$\mathrm{Tr}_{L/K}\beta=\sum_{i=1}^{n}\beta_i,\quad \mathrm{N}_{L/K}\beta=\prod_{i=1}^{n}\beta_i.$$

3. 设L是K的n次扩域，而$\beta\in L$对K的极小多项式设为

$$g(x)=x^m+b_1x^{m-1}+\cdots+b_m.$$

令$r=n/m$。证明

$$\mathrm{Tr}_{L/K}\beta=-rb_1,\quad \mathrm{N}_{L/K}\beta=(-1)^n b_m^r.$$

4. 设α是$x^3-2=0$的一个根，$K=\mathbf{Q}(\alpha)$。令$\beta=-1+\alpha-2\alpha^2$。试求$\mathrm{Tr}_{K/\mathbf{Q}}\beta$与$\mathrm{N}_{K/\mathbf{Q}}\beta$。

5. 设α是$x^3-2x+2=0$的一个根，令$K=\mathbf{Q}(\alpha)$，试求

$$\mathrm{Dis}(1,\alpha,\alpha^2).$$

6. 设D是一个无平方因子的整数，$K=\mathbf{Q}(\sqrt{D})$。试求

$$\mathrm{Dis}(1,\sqrt{D}).$$

7. 设L是域K的n次伽罗瓦扩域，其伽罗瓦群G是由σ生成的循环群，证明对$u\in L$，$\mathrm{N}_{L/K}u=1$的充分必要条件是：存在$v\in L$，使$u=v/\sigma(v)$。

8. 设L是域K的n次伽罗瓦扩域，其伽罗瓦群G是由σ生成的循环群，设$d\in L$，$\mathrm{Tr}_{L/K}d=0$，证明存在$c\in L$，使

$$d=c-\sigma(c).$$

9. 设L是有限域，K是L的子域，证明映射

$$N_{L/K}:\ L\to K$$

是L到K的满射。

§9 超越扩张

我们在讨论域的基数时，知道复数域$\boldsymbol{C}$中有许多对$\boldsymbol{Q}$的超越元。换言之，$\boldsymbol{C}$不是$\boldsymbol{Q}$的代数扩域。一般言之，任给扩域$L\supset K$，则L不一定是K的代数扩域。如果L不是K的代数扩域，则称L是K的**超越扩域**。

定义5.20 1) 设$\{x_i\}\subset L$，如果它的任意有限子集都是对K代数无关的，即不适合系数在K中的任何非零的多元多项式，则称$\{x_i\}$是一个**超越集**。

2) 如果L有一超越集$\{x_i\}$，使$L=K(\{x_i\})$，则称L是K的**纯超越扩域**。

我们有下面的有趣的定理。

定理5.34(Lüroth 定理) 设有$K(x)\supset L\supsetneqq K$，此处$x$是超越元。则必存在超越元$y$，使$L=K(y)$。

证明 任取$\alpha(x)\in L\backslash K$，设

$$\alpha(x)=\frac{r(x)}{s(x)},\quad r(x),s(x)\in K[x].$$

令Z为一变数，则x显然适合下面的方程式：

$$\alpha(Z)-\alpha(x)=0,$$

即
$$r(Z)-\alpha(x)s(Z)=0.$$

此式左端显然是$L[Z]$中的多项式，故$L[x]$是L的代数扩域，且$K(x)=L(x)$。令$m=[K(x):L]$。再设x对L的极小多项式$f(Z)\in L[Z]$为下面的形式：

$$f(Z)=Z^m+\alpha_1(x)Z^{m-1}+\cdots+\alpha_m(x),$$

其中
$$\alpha_i(x)=\frac{f_i(x)}{g_i(x)},\quad f_i(x),g_i(x)\in K[x].$$

经整理、消去上式的公分母以后，得

(1) $$h(x,Z)=h_0(x)Z^n+h_1(x)Z^{n-1}+\cdots+h_m(x).$$
其中
$$h_i(x)\in K[x]. \quad a_i(x)=\frac{h_i(x)}{h_0(x)}, \quad (h_0(x),\cdots,h_m(x))=(1).$$
显然必有某 $a_i(x)\bar{\in} K$（否则 x 是对 K 的代数元）. 令 $y=a_i(x)\bar{\in} K$.
则
$$y=\frac{h_i(x)}{h_0(x)}=\frac{a(x)}{b(x)}, \quad a(x),b(x)\in K[x],(a(x),b(x))=(1).$$
显然 x 也适合下式：

(2) $$A(x,Z)=b(x)a(Z)-a(x)b(Z)=0.$$
注意到 $h(x,Z)/h_0(x)=f(Z)\in L[Z]$, $A(x,Z)/b(x)\in L[Z]$，两者有公根 x. 而 $f(Z)$ 在 $L[Z]$ 中不可约，故
$$f(Z)\mid A(x,Z)/b(x),$$
即存在 $q(Z)\in L[Z]$，使得
$$A(x,Z)=\frac{b(x)}{h_0(x)}q(Z)h(x,Z).$$
将 $(b(x)/h_0(x))q(Z)$ 看作 $k(x)[Z]$ 中的元素，它可表示为
$$\frac{b(x)}{h_0(x)}q(Z)=k(x)r(Z) \quad ,$$
其中 $k(x)\in K(x)$, $r(Z)$ 是 $K[x][Z]$ 中的本原多项式，于是有
$$A(x,Z)=k(x)r(Z)h(x,Z).$$
由于 $A(x,Z)$, $r(Z)$, 以及 $h(x,Z)$ 都是 $K[x][Z]$ 中的本原多项式，应用高斯引理，即知 $k(x)\in K$，所以 $k(x)r[Z]\in K[x][Z]$. 令
$$B(x,Z)=k(x)r(Z),$$
则有 $k[x][Z]$ 内的等式

(3) $$A(x,Z)=B(x,Z)h(x,Z).$$
令 $n=\deg_x h(x,Z)$. 则
$$n=\sup(\deg_x h_i(x))\geqslant\sup(\deg_x a(x),\deg_x b(x))$$
$$\geqslant\deg_x A(x,Z).$$
比较(3)式两侧 x 的次数，我们立得

$$\deg_x B(x,Z)=0.$$

现在说明 $B(x,Z)$是一个常数，即 $\deg_Z B(x,Z)=0$。假若不然，则 $A(x,Z)$有一个因元 $C(Z)$。考虑(2)式，对换 x，Z，则知 $A(x,Z)$有因元 $C(x)$. 又考虑(3)式，$h(x,Z)$是 $K[x][Z]$ 的本原多项式，所以 $C(x)$必是 $B(x,Z)$的因元，与前面的结果

$$\deg_x B(x,Z)=0$$

相矛盾。

总结前述，我们得到 $B(x,Z)=B\in K$，也即

$$A(x,Z)=B\cdot h(x,Z).$$

于是立得下面的数值关系式：

$$\deg_x A(x,Z)=\deg_x h(x,Z)=n,$$

$$\deg_Z A(x,Z)=\deg_Z h(x,Z)=m.$$

显然，$\deg_x A(x,Z)=\deg_Z A(x,Z)$，故 $n=m$。而 $y=a(x)/b(x)$，故 $K(y)[Z]$中的不可约多项式

$$\frac{A(x,Z)}{b(x)}=a(Z)-yb(Z)$$

以 $Z=x$ 为根。此多项式对Z的次数为 $n=m$。由$K(y)\subset L$，即知

$$m=[K(x):L]\leqslant[K(x):K(y)]=m,$$

立得 $L=K(y)$。❙

例21　一个不可约代数曲线 $f(x,y)=0$ 称为**有理代数曲线**，如果存在参数式

$$x=\alpha(t),\quad y=\beta(t),\quad \alpha(t),\beta(t)\in K(t),$$

使得 $f(\alpha(t),\beta(t))=0$。令 L 为 $K[x,y]/(f(x,y))$ 的比域，应用上面的 Lüroth 定理(参看本节习题 7)，则立得

$$L=K(t'),$$

其中 t' 为 $K(t)$中一适当的超越元。

我们把上面的道理应用到积分学上：求下面的积分

$$\int f(\cos\theta,\sin\theta)\mathrm{d}\theta.$$

令 $x=\sin\theta$，$y=\cos\theta$，则 x，y 适合下式

$$x^2+y^2=1.$$

此式定义的是单位圆。我们来求x，y的有理参数表示。以点 (0,1) 为投影中心，作图5.5所示的投影，则不难算出

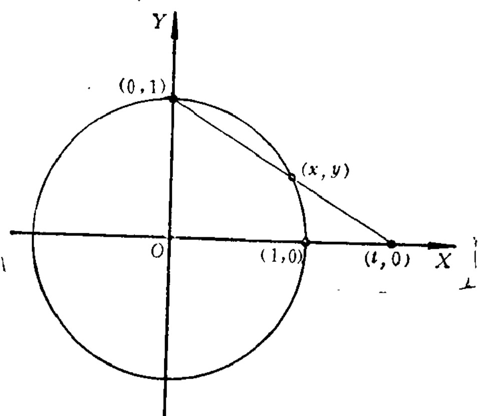


图 5.5

$$x=\frac{2t}{t^2+1},$$

$$y=\frac{t^2-1}{t^2+1}.$$

易知

$$\mathrm{d}\theta=\frac{1}{y}\mathrm{d}x,$$

故

$$\mathrm{d}x=\frac{2-2t^2}{(t^2+1)^2}\mathrm{d}t.$$

代入原积分式，即得

$$\int f(\sin\theta,\cos\theta)\,\mathrm{d}\theta=\int g(t)\mathrm{d}t,$$

其中 $g(t)$ 为 t 的有理函数。于是，三角函数的积分就归结成有理函数的积分了。

例22 并不是所有的代数曲线都是有理代数曲线。我们举一例说明之。令 $x^n+y^n-1\in\boldsymbol{C}[x,y]$，此处 $n>2$。我们要证明，这不是一个有理代数曲线。

假设有

$$x=\frac{a(t)}{b(t)},\quad y=\frac{c(t)}{d(t)},\quad a(t),b(t),c(t),d(t)\in\boldsymbol{C}[t],$$

使得

$$\frac{a(t)^n}{b(t)^n}+\frac{c(t)^n}{d(t)^n}-1=0.$$

通分，消去公因元之后，立得

$$f(t)^n+g(t)^n=h(t)^n, \tag{1}$$

其中 $f(t),g(t),h(t)\in \mathbf{C}[x],(f(t),g(t),h(t))=(1)$，且 $f(t)$，$g(t),h(t)$中最少有一个不是常数。我们要说明这是不可能的。假若有三个多项式满足上述条件，我们无妨假定(1)式中的$f(t)$，$g(t),h(t)$的最高次数

$$\max\{\deg f(x),\deg g(x),\deg h(x)\}$$

是所有满足上述条件的三个多项式的最高次数中的最小者。因为 $\mathbf{C}$ 中含有 -1 的 n 次方根，所以又不妨设

$$\deg h(x)\geqslant \deg f(x),\deg g(x).$$

令 ω 为 n 次单位根，则(1)式可改写成

$$\prod_{i=1}^{n}(f(t)+\omega^i g(t))=h(t)^n. \tag{2}$$

由于 $f(t)+\omega^i g(t)$ 与 $f(t)+\omega^j g(t)$ $(i\neq j)$ 的公因元必是 $f(t)$与$g(t)$的公因元，因此也是 $h(t)$ 的因元，所以 $f(t)+\omega^i g(t)$ 与 $f(t)+\omega^j g(t)$必互素。令

$$f(t)+\omega^i g(t)=h_i(t),\quad i=1,2,\cdots,n, \tag{3}$$

则$(h_i(t),h_j(t))=(1)$ $(i\neq j)$. 又有$\prod\limits_{i=1}^{n}h_i(t)=h(t)^n$，故必有

$$h_i(t)=\alpha_i(t)^n,\quad \alpha_i(t)\in\mathbf{C}[t]. \tag{4}$$

将(4)式代入(3)式，由对应于 $i=1,2,3$ 的三个式子中消去 $f(x)$，$g(x)$，我们立得

$$\varepsilon_1\alpha_1(t)^n+\varepsilon_2\alpha_2(t)^n=\varepsilon_3\alpha_3(t)^n,$$

其中 $\varepsilon_1,\varepsilon_2,\varepsilon_3\in\mathbf{C}$。令 $\beta_i(t)=\sqrt[n]{\varepsilon_i}\,\alpha_i(t)$ $(i=1,2,3)$，则

$$\beta_1(t)^n+\beta_2(t)^n=\beta_3(t)^n.$$

显然有

$$\max\{\deg\beta_1(t),\deg\beta_2(t),\deg\beta_3(t)\}$$
$$<\max\{\deg f(t),\deg g(t),\deg h(t)\}.$$

又由(3)式不难看出 $h_i(t)(i=1,2,\cdots,n)$ 中最多只能有一个是常数，故 $\beta_1(t),\beta_2(t),\beta_3(t)$ 不全是常数。这与我们开始时对 $f(t)$，$g(t),h(t)$ 的假设相矛盾。

讨论 Lüroth 定理能不能推广到二元或多元的情形？我们现在所知道的有：

Zariski-Castelnuovo 定理 设 K 是特征为零的代数封闭域，则任何 $K(x,y)\supset L\supsetneqq K$ 可以写成 $L=K(u)$ 或 $K(u,v)$，此处 u，v 是代数无关的。

如果 K 的特征不是零时，则有反例。又在三元时，类似的结果并不成立，也有反例(如Cleimens-Griffiths, Iskovskiv-Manin, M.Artin-Mumford 等的反例)。 ▎

以下我们讨论 L 对 K 的"超越次数"。这与关于向量空间的维数的讨论是很相像的。从更高一层的抽象来看，两者是完全一致的。

定义 5.21 给定 L 的一个子集 $\{x_i\}$。如果 L 是 $K(\{x_i\})$ 的代数扩域，则称 $\{x_i\}$ 是 L 的**生成集**。

定义 5.22 如果 $\{x_i\}\subset L$ 是对 K 的一个超越集，又是一个生成集，则称 $\{x_i\}$ 为 L 对 K 的**超越基**。

讨论 在向量空间中，与这里"代数无关"(超越集的定义 5.19中)、"$K(\{x_i\})$"、"超越基"相对应的分别是"线性无关"、"$\{x_i\}$ 生成的子空间"、"基"。 ▎

如同在向量空间的讨论中一样，我们考虑下面这个简单的情形。

定理 5.35 设 $\{x_1,x_2,\cdots,x_n\}$ 是 L 对 K 的一个超越基。又设 $\{y_i\}$ 是 L 对 K 的另一个超越基，则 $\{y_i\}$ 有 n 个元素。

证明 证法与向量空间讨论维数时所用的"替换"方法是一

样的。任取 y_j，则 y_j 是对 $K(x_1,\cdots,x_n)$的代数元。于是存在系数取自K的 $n+1$ 元非零多项式 f，使

$$f(x_1,\cdots,x_n,y_j)=0,$$

在此多项式中，必有一个 x_i 出现。我们要用 y_j 替换 x_i，即证明

$$\{x_1,\cdots,\hat{x}_i,\cdots,x_n\}\cup\{y_j\}$$

也是超越基。证法如下：

1) 先证L是$K(x_1,\cdots,x_{i-1},x_{i+1},\cdots,x_n,y_j)$的代数扩域。事实上，$L$是$K(x_1,\cdots,x_n,y_j)$的代数扩域，$K(x_1,\cdots,x_n,y_j)$又是$K(x_1,\cdots,x_{i-1},x_{i+1},\cdots,x_n,y_j)$的代数扩域。所以1)得证。

2) 再证$\{x_1,\cdots,x_{i-1},x_{i+1},\cdots,x_n,y_j\}$是超越集。假若不然，设

$$g(x_1,\cdots,x_{i-1},x_{i+1},\cdots,x_n,y_j)=0,$$

自然，y_j 必然出现，于是L是$K(x_1,\cdots,x_{i-1},x_{i+1},\cdots,x_n)$的代数扩域，也即 x_i 是对$K(x_1,\cdots,x_{i-1},x_{i+1},\cdots,x_n)$的代数元，立得$\{x_1,\cdots,x_n\}$不是超越集。

建立了上述的替换方法后，我们取 y_1 替换 x_i，不妨设 $i=1$。于是$\{y_1,x_2,\cdots,x_n\}$是一个超越集。我们再用 y_2 替换$\{y_1,x_2,\cdots,x_n\}$的元素时，考虑方程式

$$f(y_1,x_2,\cdots,x_n,y_2)=0.$$

此式中必含有 $x_2,\cdots,x_n$ 之一(否则 f 成为 y_1 与 y_2 适合的多项式了，这与 y_1,y_2 代数无关相矛盾)。因此我们可以用 y_2 替换某个 $x_k(k\geqslant 2)$，不妨即设 $k=2$。反复如此作下去，立得

$$n=\{x_i\}\text{的基数}\geqslant\{y_j\}\text{的基数}.$$

于是二者必然相等。▌

讨论 在一般情形下，L的任何两个超越基都有相同的基数。其证法不难，只是较繁而已。所以本书不引入。

定义5.23 L对K的**超越次数**定义为超越基的基数，用符号 $\operatorname{tr}\deg(L/K)$表示之。

习　题

1. 设 L 是 K 的扩域，$K\subset F\subset L$。如果

$$\operatorname{tr\,deg}(F/K)=s,\quad \operatorname{tr\,deg}(L/F)=t.$$

证明 $\operatorname{tr\,deg}(L/K)=s+t$。

2. 设 $k(x)$ 是 k 的单超越扩张，$u\in k(x)$。证明 $k(x)=k(u)$ 的充要条件是

$$u=\frac{ax+b}{cx+d},\quad a,b,c,d\in k,\ ad-bc\neq 0.$$

3. 设 $k(x)$ 是 k 的单超越扩张，n 是正整数。证明存在 $k(x)$ 的 n 次扩域 K，使 K 对 k 仍为单超越扩张。

4. 设 k 是域，$f(x),g(x)\in k[x]$，$\deg f(x)=m$，$\deg g(x)=n$。又设 $k(u)$ 是 k 的一单超越扩张，令 $\alpha=f(u)$，$\beta=g(u)$。证明 α,β 满足一个对 α 为 n 次，对 β 为 m 次的方程式。

5. 设 L 是域 K 的扩域，E_1,E_2 是两个中间域。证明：

$\operatorname{tr\,deg}(E_1E_2/K)\geqslant\operatorname{tr\,deg}(E_i/K)\quad(i=1,2)$，

$\operatorname{tr\,deg}(E_1E_2/K)\leqslant\operatorname{tr\,deg}(E_1/K)+\operatorname{tr\,deg}(E_2/K)$。

6. 设 S 是复数域 $\mathbf{C}$ 对 $\mathbf{Q}$ 的超越基，证明 S 是无限集。

7. 设 $f(x,y)$ 是 $K[x,y]$ 的不可分解元，并且存在 $\alpha(t)$，$\beta(t)\in K(t)$，使得 $f(\alpha(t),\beta(t))=0$。定义 $K[x,y]$ 到 $K(t)$ 的映射

$$\varphi:\ g(x,y)\mapsto g(\alpha(t),\beta(t)).$$

证明 φ 引生出 $K[x,y]/(f(x,y))$ 到 $K(t)$ 的环单射，从而推知 $K[x,y]/(f(x,y))$ 的比域 L 可以嵌入 $K(t)$ 作为其子域。

附录　自然数的皮诺公理系

自然数0，1，2，…是人们早已熟知的，但由于它在数学中起着重要的作用，我们有必要从逻辑上给出它的严格定义。在这个附录中，我们介绍一下皮诺(Peano)的自然数公理体系。

定义　设$\boldsymbol{N}$是一非空集合，而且：

1）在$\boldsymbol{N}$内存在一个特定元素，记作0；

2）存在$\boldsymbol{N}$到自身的一个映射，记作$n \mapsto n^{+}$，称为**后继映射**，使下面三条公理满足：

(a)　对任意$n \in \boldsymbol{N}$，$n^{+} \neq 0$；

(b)　$n \mapsto n^{+}$是一个单射；

(c)　(归纳公理)$\boldsymbol{N}$的一个子集T如具备如下条件：

i)　$0 \in T$；

ii)　若$n \in T$，则$n^{+} \in T$，那么，必定有$T=\boldsymbol{N}$。

此时，称$\boldsymbol{N}$是一个**自然数系**，$\boldsymbol{N}$内的元素称为**自然数**。

从自然数系定义中的归纳公理，我们立得如下重要的原理。

第一归纳原理　如果每个自然数n都对应于某个命题$E(n)$。当已知：1）命题$E(0)$成立；2）若命题$E(n)$成立，则命题$E(n^{+})$必定也成立，此时即可断定命题$E(n)$对一切自然数n都成立。

证明　以T表示使命题$E(n)$成立的所有自然数n所成的集合。按假设，$0 \in T$，且若$n \in T$，则$n^{+} \in T$。于是按照归纳公理，

$$T=\boldsymbol{N}. \quad \blacksquare$$

上面所述的第一归纳原理，就是我们常用的数学归纳法的理论依据。

下面我们再从$\boldsymbol{N}$的定义出发，在$\boldsymbol{N}$内定义加法、乘法，并使它们满足我们习以为常的一些运算规律。为此，我们先来证明

一个定理.

递归定理 令S是一个集合，φ是S到自身的一个映射，a是S的一个固定元素。那么，存在$\boldsymbol{N}$到S的唯一的映射f，满足如下条件：

1） $f(0)=a$；

2） $f(n^{+})=\varphi(f(n))$.

证明 我们考察集合$A=\{(n,s): n\in\boldsymbol{N}, s\in S\}$. 设$\Gamma$是由具有下列性质的$A$的子集$U$所成的集合：

1） $(0,a)\in U$；

2） 若$(n,b)\in U$，则$(n^{+},\varphi(b))\in U$.

显然，$A\in\Gamma$，故$\Gamma\neq\varnothing$. 命F为Γ内所有集合的交集，我们有$(0,a)\in F$，故$F\neq\varnothing$. 下面证明F的两条基本性质.

1） $\forall n\in\boldsymbol{N}$，必存在$b\in S$，使$(n,b)\in F$. 这是因为：令

$$T=\{n\in\boldsymbol{N}: \text{存在 } b\in S, \text{使}(n,b)\in F\},$$

则已知$0\in T$. 又若$n\in T$，即存在$b\in S$，使$(n,b)\in F$，则(n,b)属于Γ的任一元素U. 于是$(n^{+},\varphi(b))$属于Γ的一切元素U，亦即$(n^{+},\varphi(b))\in F$. 于是$n^{+}\in T$. 按归纳公理，$T=\boldsymbol{N}$.

2） 若$(n,b)\in F$，$(n,b')\in F$，则必有$b=b'$. 证法如下：令

$$T=\{n\in\boldsymbol{N}: \text{若}(n,b), (n,b')\in F\Longrightarrow b=b'\}.$$

先证明$0\in T$. 已知$(0,a)\in F$. 若有$(0,a')\in F$，但$a'\neq a$. 从F中去掉$(0,a')$，得到A的子集F'. 显然$F'\in\Gamma$，故$F'\supsetneqq F$. 但已知F'为F的真子集，矛盾. 故必有$a'=a$. 即$0\in T$. 再证明：若$n\in T$，则$n^{+}\in T$. 用反证法. 如果$n^{+}\notin T$，取$(n,b)\in F$，此时$(n^{+},\varphi(b))\in F$，同时应有$c\neq\varphi(b)$，使$(n^{+},c)\in F$. 从F中去掉(n^{+},c)得到子集F'. 不难验证$F'\in\Gamma$. 从而$F'\supsetneqq F$. 这样导出矛盾. 根据归纳公理，即有$T=\boldsymbol{N}$.

现在定义$\boldsymbol{N}$到S的映射f如下：若$(n,b)\in F$，则令$f(n)=b$. 显然有

1） $f(0)=a$；

2） $f(n^+)=\varphi(f(n))$。

如果另有 $\boldsymbol{N}$ 到 S 的映射 g 也满足定理要求，则利用归纳公理可知，对一切 $n\in\boldsymbol{N}$，都有 $g(n)=f(n)$，即 $g=f$。这表示 f 是满足定理要求的唯一的映射。▎

（一）$\boldsymbol{N}$ 内的加法运算

任取 $m\in\boldsymbol{N}$，在递归定理中，取 $S=\boldsymbol{N}$，$a=m$，φ 为后继映射。我们得到 $\boldsymbol{N}$ 到 $\boldsymbol{N}$ 的一个映射 f_m。此时，对任一 $n\in\boldsymbol{N}$，定义

$$n+m=f_m(n),$$

称上式为 $\boldsymbol{N}$ 内的加法运算。

$\boldsymbol{N}$ 内的加法运算满足如下运算规律：

1） $\forall n\in\boldsymbol{N}$，$n+0=n$；

2） 交换律：$n+m=m+n$；

3） 结合律：$(m+n)+l=m+(n+l)$；

4） 消去律：$m+n=l+n\Longrightarrow m=l$。

上面这些运算律都可以从逻辑上给以严格的证明。我们只举两个例子。

1)的证明 按定义，我们应证明 $f_0(n)=n$。令

$$T=\{k\in\boldsymbol{N}:\ f_0(k)=k\}.$$

因 $f_0(0)=0$，故 $0\in T$。若 $k\in T$，则 $f_0(k)=k$。于是

$$f_0(k^+)=[f_0(k)]^+=k^+,$$

故 $k^+\in T$。按归纳公理，$T=\boldsymbol{N}$。▎

2)的证明 我们先证明 $f_{n^+}(k)=[f_n(k)]^+$。为此，令

$$T=\{k\in\boldsymbol{N}:\ f_{n^+}(k)=[f_n(k)]^+\}.$$

首先，因为 $f_{n^+}(0)=n^+=[f_n(0)]^+$，故 $0\in T$。其次，设 $k\in T$，即

$$f_{n^+}(k)=[f_n(k)]^+.$$

那么，我们有（利用递归定理中映射 f 的性质）

$$f_{n^+}(k^+)=[f_{n^+}(k)]^+=\{[f_n(k)]^+\}^+=\{f_n(k^+)\}^+,$$

即 $k^+\in T$。于是按归纳公理，$T=\boldsymbol{N}$。

现在取定 $m\in\boldsymbol{N}$。令

$$T=\{n\in\boldsymbol{N}:\ f_m(n)=f_n(m)\}.$$

因 $f_m(0)=m=f_0(m)$，故 $0\in T$。设 $k\in T$，我们有

$$f_m(k^+)=[f_m(k)]^+=[f_k(m)]^+=f_{k^+}(m).$$

即 $k^+\in T$，故 $T=\boldsymbol{N}$。这表明对任意的 $m, n\in\boldsymbol{N}$，我们都有

$$m+n=n+m. \quad \blacksquare$$

（二）$\boldsymbol{N}$ 内的乘法运算

任取 $m\in\boldsymbol{N}$，在递归定理中，取 $S=\boldsymbol{N}$，$a=0$，φ 为映射：$n\mapsto n+m$。于是我们得到 $\boldsymbol{N}$ 到自身的一个映射 f^m。对任意的 $n\in\boldsymbol{N}$，定义

$$nm=f^m(n),$$

称上式为 $\boldsymbol{N}$ 内的**乘法运算**。

$\boldsymbol{N}$内的乘法满足如下运算律：

1）$0\cdot m=0$；

2）交换律：$mn=nm$；

3）结合律：$(mn)l=m(nl)$；

4）消去律：$mn=ln$，$n\neq 0\Longrightarrow m=l$；

5）分配律：$l(m+n)=lm+ln$。

上面各条运算律的证明从略。

（三）$\boldsymbol{N}$内的序

任给 $m,n\in\boldsymbol{N}$。如存在 $x\in\boldsymbol{N}$，使 $m=n+x$，则定义 $m\geqslant n$（或写成 $n\leqslant m$）。于是有

1）$m\geqslant n$，$n\geqslant m\Longleftrightarrow m=n$；

2）若 $m\geqslant n$，$n\geqslant l$，则 $m\geqslant l$；

3）对任意的m，$n\in \boldsymbol{N}$，$m\geqslant n$或$n\geqslant m$，二者必有一成立；

4）$\boldsymbol{N}$的任一非空子集S中都存在最小自然数，即存在$l\in S$，使$\forall m\in S$有$m\geqslant l$；

5）若$m\geqslant n$，则$m+l\geqslant n+l$；

6）若$m\geqslant n$，则$ml\geqslant nl$。

上面各条的证明也从略。

有了上述三个方面的结果，我们所熟悉的自然数的一些基本知识都从逻辑上严格地确立起来了。

汉英名词索引

一　画①

二　画

三　画

① 凡英文字母开始的词汇都并入一画之内。

四　画

五　画

六　画

七　画

八　画

九　画

十　画

十 一 画

十 二 画

十 三 画

十 四 画

十 六 画